Crypto News

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

July 06, 2025

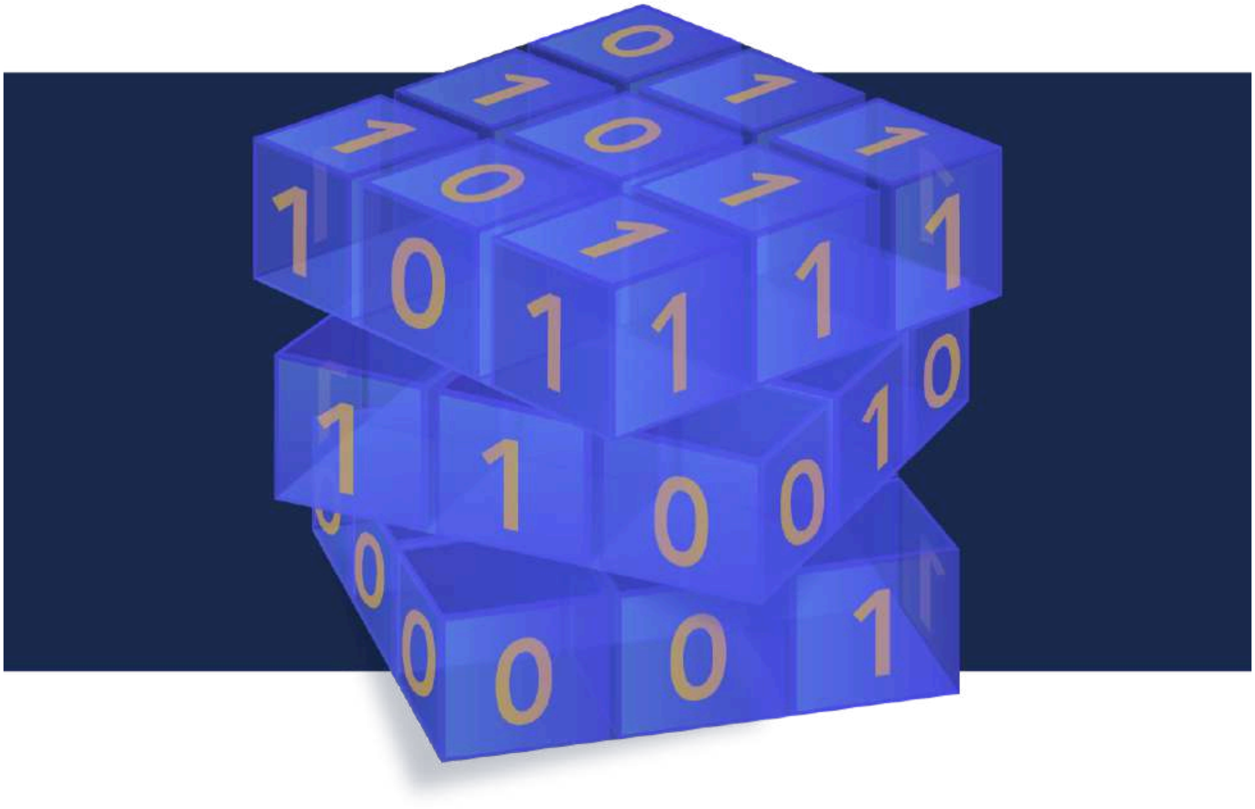


Table of Contents

Editorial

Summer's here—late sunsets, cold drinks, and the sweet freedom to do absolutely nothing (or everything). While you do whatever it is that your heart desires, let's catch up on all things quantum while taking in these beautiful summer days. If you want to know about which cybersecurity start-ups are taking the lead in quantum preparedness, scroll down just a bit to article 1. If you're a part of our working group, you'll likely recognize some of the company names since some of our members are affiliated with them. As quantum computing threatens to render current encryption obsolete, cybersecurity startups like QNu Labs, Pantherun Technologies, and Nu Quantum are developing advanced tools—from AI-driven encryption to single-photon systems—to protect future digital infrastructure. Switzerland's ID Quantique delivers quantum key distribution and fast encryption for global networks, while QuintessenceLabs provides quantum-grade random number generation and key management for cloud and mobile security. Suffice to say, we should applaud these 5 organizations, amongst others, who are working towards a quantum-safe future that many in the world may not yet know they need.

China's announcement of the ez-Q Engine 2.0 in article 14, is described as a 1,000-qubit quantum computer. This, however, is an inaccurate representation as it is actually a quantum computer controller designed to manage qubits rather than a fully operational quantum processor. While this represents progress in quantum control technology, it is not a 1,000-qubit quantum computer as it was so widely reported. This is yet another reminder for all of us to always remain vigilant and properly vet the news we ingest. It is noted though that China is putting a lot of money into the quantum arms race and making progress. While some countries are actively advancing their quantum technologies, others are doing the same but are also focused on preparing for a quantum future. Articles 2, 12, and 18 highlight how Canada, the EU, and India respectively, are each taking steps towards quantum-safe encryption on critical systems to protect sensitive, private, and nation critical information from the threats posed by quantum computing. Although their approaches and timelines may slightly differ, all three share a common commitment to starting now and not waiting to respond to the impending quantum threat. If they aren't waiting, then your companies shouldn't be either.

As always, this newsletter has many other articles worth your attention so dive right in. Happy Reading!

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

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

1. 5 cybersecurity startups strengthening digital defences against quantum threats

by Staff Writer
https://www.manufacturingtodayindia.com/5-cybersecurity-startups

Quantum computers are no longer a sci-fi concept; they are becoming a reality, bringing with them a new type of cybersecurity threat. The sheer power of quantum computing might make traditional encryption techniques, which safeguard everything from financial information to national security systems, obsolete. There has never been a greater need for quantum-resilient cybersecurity as this technological revolution draws near.

India is rising to the occasion. Alternative security solutions are being developed by a new generation of domestic businesses. In order to safeguard data in a future where current algorithms might not be sufficient, these pioneers are creating post-quantum cryptographic tools, secure communication channels, and quantum-safe encryption.

Here are 5 Indian cybersecurity startups leading the charge to secure our digital future in the quantum age.

1. QNu Labs (Bengaluru)

QNu Labs is one of the first Indian companies to build cybersecurity products using quantum technology. Their tools help keep data safe on the internet and in the cloud—even from future threats that today's systems can't handle.

The company was started with a strong belief that India can build world-class tech products. Today, QNu Labs is solving modern cybersecurity problems using the power of quantum science. The team is made up of passionate experts in quantum physics, cybersecurity, optoelectronics, laser technology, and high-precision electronics. QNu Labs is proud to be India's first—and only—quantum cryptography company, placing the country firmly on the global quantum technology map.

2. Pantherun Technologies

Pantherun Technologies is a Bengaluru-based cybersecurity company that's changing the way data is protected—at the chip and software level. With a patented encryption technology that works in real time, Pantherun makes it 10x harder for attackers to breach systems. What's more, their solution is built to resist the future threats of quantum computing and side-channel attacks.

Pantherun's unique approach doesn't need key exchange or format changes. It uses AI to generate encryption keys independently at both ends of a communication line, making it extremely secure and easy to integrate across devices. From Ethernet ports in cars to sensors in smart cities, Pantherun's technology protects data across critical industries

3. Nu Quantum

Nu Quantum is a cutting-edge startup specialising in quantum cryptography systems. The company develops modular hardware rooted in single-photon source array technology to power the next generation of quantum-secure communication. Its solutions include a quantum random number generator for creating unbreakable encryption keys and a quantum key distribution (QKD) system to enable ultra-secure data transfer.

Led by co-founders Carmen Palacios-Berraquero and Matthew Applegate, Nu Quantum has secured $12.1 million in funding from top-tier investors like Amadeus Capital, IQ Capital, and Expeditions Fund, with a current valuation of £9.43 million. The company operates in a competitive space with over 200 players, standing out alongside peers like QNu Labs, QuintessenceLabs, and ID Quantique.

4. ID Quantique

Founded in 2001 in Geneva, Switzerland, ID Quantique (IDQ) is a pioneer in network and data encryption, leveraging quantum technologies to secure sensitive information. The company offers high-performance network encryption solutions capable of protecting data in transit at speeds of up to 100Gbps, ideal for data centre interconnects and global WAN networks.

IDQ integrates quantum key generation and quantum key distribution (QKD) to ensure long-term data protection against emerging cyber threats. Backed by investors like SK Telecom and Quantum Wave Fund, the company has raised $10.8 million to date.

5. QuintessenceLabs

QuintessenceLabs is a Series B company delivering advanced quantum encryption-based data security solutions. Its product suite includes quantum true random number generators, enterprise key and policy managers, and a vendor-neutral SDK for seamless integration.

The company's technologies enable file encryption across cloud, network, and mobile environments, with a focus on high-assurance random number generation and robust key management.

2. Canada Sets Timeline to Shield Government Systems from Quantum Threat

by Matt Swayne
https://thequantuminsider.com/2025/06/28/canada-sets-timeline-to-shield-government-systems-from-quantum-threat/

The Canadian government has launched a formal plan to protect its federal IT infrastructure from the looming risks posed by quantum computers, setting strict milestones through 2035 for a nationwide migration to post-quantum cryptography.

Detailed in a roadmap published by the Canadian Centre for Cyber Security, the initiative mandates all federal departments to adopt encryption standards that are resistant to attacks from quantum machines. These computers, once powerful enough, could render many current encryption methods obsolete, potentially exposing sensitive government data to future decryption.

The strategy, effective as of June 23, 2025, sets out clear deadlines. Federal departments must submit an initial post-quantum cryptography (PQC) migration plan by April 2026 and continue reporting annually. High-priority systems must complete migration by the end of 2031, with all remaining systems transitioned by 2035. The roadmap applies to non-classified systems and includes IT infrastructure managed both internally and through third-party services, such as cloud providers.

The Cyber Centre, Canada's lead authority on IT security and part of the Communications Security Establishment, issued the plan in partnership with Shared Services Canada (SSC) and the Treasury Board Secretariat (TBS). The roadmap aligns with global standards being finalized by the U.S. National Institute of Standards and Technology (NIST) and supports Canada's broader National Quantum Strategy.

According to the guidance, departments are expected to identify all systems currently relying on vulnerable public-key encryption—used for securing communications, authenticating users, and other functions. The risk isn't just theoretical and not just a threat set in the vague future. The roadmap warns that hostile actors may already be collecting encrypted data with the intent to decrypt it later when quantum computing becomes viable, a strategy known as "harvest now, decrypt later."

Departments must first carry out a comprehensive audit to locate all instances of cryptographic usage. This includes everything from server racks and laptops to smart cards, printers, and voice-over-IP phones. The aim is to build a full inventory of components using at-risk encryption, identifying those most critical and vulnerable.

To coordinate the transition, each department must appoint a PQC migration executive lead from senior management, supported by a technical lead and a cross-functional committee. These teams are responsible not only for planning and execution but also for educating staff on quantum risks, budgeting for system upgrades, and integrating PQC into procurement policies.

The Cyber Centre cautions that not all existing systems can be retrofitted. Some legacy systems may require full replacement, while others might be protected in the interim through secure tunneling or network isolation. The roadmap emphasizes that early planning is essential to avoid rushed procurement and higher costs.

The transition phase will rely heavily on identifying which products and services can be upgraded and which must be replaced. The guidance encourages departments to engage vendors early to confirm PQC roadmaps and product compatibility. Some cryptographic modules will need to be certified through recognized programs, and new purchases must allow for cryptographic flexibility to adapt to evolving standards.

The Cyber Centre will provide further technical assistance through its sensor programs and network monitoring tools. It also plans to update network protocol configuration guidance and maintain a shared resource repository via the TBS GCxchange platform.

Governance of the initiative will be coordinated by the IT Security Tripartite—a joint body comprising the Cyber Centre, SSC, and TBS—which will oversee progress, manage compliance, and issue additional guidance. Departments are also subject to oversight by the Government of Canada's Enterprise Architecture Review Board, which ensures new systems meet cybersecurity and digital service standards.

Progress reports will be integrated into the federal digital services planning process. The government intends these reports to ensure transparency and help departments adjust timelines and resources as needed.

3. Amaravati to Host India's First Quantum Computing Valley

by P. Sujatha Varma
https://www.thehindu.com/news/national/andhra-pradesh/amaravati-to-host-indias-first-quantum-computing-valley/article69735727.ece

The first Quantum Computing Valley of India will be launched in Amaravati by January 2026, marking a major milestone in the country's quantum technology journey, Secretary, Information Technology, Electronics and Communications (ITE & C) Katamneni Bhaskar has said.

Speaking at a workshop on Amaravati Quantum Valley on Wednesday, he said not only Andhra Pradesh, but also educational institutions, healthcare providers, pharma companies, agri-tech, and med-tech industries across the country will be able to utilise the services of the Quantum Valley.

The Amaravati Quantum Valley Tech Park would provide scope for lakhs of professionals to work, contributing to research, innovation, and industrial growth, he said.

"States, government bodies, and institutions from across the country will have access to its infrastructure and services. Our goal is to ensure that quantum technology benefits all of human society," Mr. Bhaskar said.

Refuting the apprehensions that quantum computing would eliminate jobs, he said, "This technology is not a replacement for humans. Traditional computers will continue to play their role. Quantum computing is meant to solve problems and conduct research that are otherwise impossible or time-consuming with classical systems."

"The project is expected to create vast employment opportunities and encourage startups. To equip youth with the necessary skills, the government is collaborating with the Ratan Tata Innovation Hub, offering training and upskilling programmes," he said.The Amaravati Quantum Valley Centre will operate in alignment with the goals of the National Quantum Mission, aiming to increase productivity and create wealth through advanced technologies.

Member of the National Quantum Mission (NQM) and advisor to TCS, Anil Prabhakar, said major global companies such as IBM and Google were already engaged in research on quantum computers in the country. Quantum computing technology was being applied in fields such as pharmaceutical research, EV battery development, bin packing, cargo delivery, route optimisation and image classification, he said.

On the security front, he said, the Central government was implementing the 'QNu Project' (Quantum Secure Communication Network) to ensure the safety of computing networks and password security using quantum technology.

Director, IBM Research India Amit Singhee said quantum computing is becoming crucial in logistics, space, pharmaceuticals, education, healthcare, financial services and cyber security. "By 2029, IBM will deliver Quantum Starling, a large-scale, fault-tolerant quantum computer. In line with this, IBM has entered into an agreement to establish logical qubit quantum computers in Amaravati," he said.

Principal Director and Research Lead at LTI-Mindtree A. Vijay Rao said use of quantum AI and related technologies were being explored for monitoring of financial transactions, sequential number generation, logistics management, supply chain optimisation, manufacturing, healthcare, and robotics.

Speaking about the growing relevance of quantum computing in risk analysis, climate change modelling, cryptographic optimisation and more, he said LTIMindtree was joining hands with IBM and TCS as a key partner in the Amaravati Quantum Valley Centre to build solutions, develop talent and drive innovation.

4. F5 launches post-quantum cryptography solutions for app security

https://in.investing.com/news/company-news/f5-launches-postquantum-cryptography-solutions-for-app-security-93CH-4891078

F5, a technology company with impressive gross profit margins of 81% and an excellent financial health rating according to InvestingPro, has introduced new post-quantum cryptography (PQC) readiness solutions integrated into its Application Delivery and Security Platform, the company announced in a press release.

The solutions aim to help organizations prepare for cybersecurity challenges posed by quantum computing, which experts predict will make current asymmetric cryptography vulnerable by 2029 and "fully breakable" by 2034.

F5's PQC offerings provide both server-side and client-side encryption capabilities that work across hybrid, multi-cloud, and legacy environments. The company's approach combines classical encryption with post-quantum methods to enable gradual system upgrades without business disruptions.

"Post-quantum threats aren't a distant problem—they're a forcing function to modernize security now," said Kunal Anand, Chief Innovation Officer at F5.

The company highlighted that malicious actors are already employing "harvest now, decrypt later" strategies, collecting encrypted data today with plans to decrypt it when quantum capabilities become available.

F5's solutions implement NIST-standardized cryptographic algorithms and provide full proxy capabilities that allow organizations to adopt hybrid cryptographic models at their own pace. The platform also offers visibility into encrypted traffic to enhance threat detection during the transition to quantum-safe protocols.

The PQC readiness solutions are currently available for the F5 Application Delivery and Security Platform. The company positions these offerings as helping businesses meet evolving regulatory standards while maintaining operational continuity during the transition to quantum-safe security measures. For deeper insights into F5's market position and comprehensive financial analysis, investors can access detailed Pro Research Reports available on InvestingPro, which covers over 1,400 top US stocks with expert analysis and actionable intelligence.

In other recent news, F5 Networks has reported strong financial results for the second quarter of 2025, exceeding analyst expectations with earnings per share (EPS) of $3.42 and revenue of $731 million. The company demonstrated a 7% year-over-year increase in total revenue, driven by a 27% rise in systems revenue and a 12% increase in product revenue. F5 Networks has also raised its full-year revenue growth guidance to 6.5-7.5%, reflecting confidence in its product offerings and market demand. Needham initiated coverage of F5 Networks with a Buy rating and a price target of $320, citing favorable second-quarter results and strong third-quarter guidance. Meanwhile, Goldman Sachs maintained a Neutral stance with a $300 price target, acknowledging the company's earnings beat but noting a flat performance in Software revenue. Additionally, F5 has integrated NGINX Plus with Red Hat Enterprise Linux to achieve FIPS compliance, now available on AWS Marketplace, enhancing security for government and other sensitive sectors. In collaboration with NVIDIA, F5 has also introduced new capabilities for its BIG-IP Next for Kubernetes platform, aimed at improving AI infrastructure efficiency and security.

5. Surging Investments in AI Are Transforming Cybersecurity

by Chuck Brooks
https://www.forbes.com/sites/chuckbrooks/2025/06/27/surging-investments-in-ai-are-transforming-cybersecurity/

AI is transforming cybersecurity, and investments are following in close concert with those trends. AI systems seek to replicate human traits and computational capabilities in a machine and surpass human limitations and speed. Elements of AI emergence consist of machine learning and natural language processing. Today, AI can understand, diagnose, and solve problems from both structured and unstructured data—and in some cases, without being specifically programmed.

AI is becoming integral in cybersecurity, and companies are logically investing in AI-based defenses against cyberattacks, and the demand for them is expected to grow in the next few years. AI offers a logical collection of tools and the best chance for defenders that work in an environment characterized by an uneven threat level and are already short on workforce and money. The demand for AI is growing due to expanded risks and threats to enterprises.

This is unambiguous evidence that AI is becoming increasingly important in cybersecurity, and organizations must capitalize on its potential to remain competitive.

The global market for AI in cybersecurity is surging. McKinsey & Company predicts a $5 to $7 trillion potential economic impact by this year. McKinsey says that AI is making the $2 trillion cybersecurity market even larger.

In the first quarter of 2024, venture capital financing for cybersecurity firms, particularly those focused on AI security solutions, experienced significant growth. According to figures from Crunchbase, startups raised over $2.7 billion in 154 deals.

From January 1 to May 5, 2024, private equity and venture capital firms said they will spend $8.1 billion on cybersecurity companies. That's a 91% rise from the same time in 2023, when it was $4.46 billion. Major cybersecurity investments in 2024.

The sums invested are going up for a solid reason. Eighty-eight percent of cybersecurity specialists said that AI will be needed to make security tasks more efficient. The Real-World Impact of AI on Cybersecurity Professionals And 62% of businesses are using or looking into AI for cybersecurity. Cybersecurity professionals have mixed feelings about AI: 93% are afraid of threats from AI, while 69% think it is the answer. In the next several years, AI's ability to change things is likely to have a big effect on the industry. 33+ AI in Cybersecurity Statistics for 2025: Friend or Foe?

"The promise of these technologies is very exciting. Microsoft UK's chief envisioning officer Dave Choplin claimed that AI is "the most important technology that anybody on the planet is working on today." R&D and investments are a good barometer of what lies ahead in future technological developments. Microsoft Exec: 'AI Is the Most Important Technology That Anybody on the Planet Is Working on Today' - Business Insider.

Smart Cybersecurity

AI has much to offer cybersecurity, both in terms of new features and in terms of improving defensive operations in contexts where threats are present. As sensors and algorithms come together, automated cybersecurity solutions for threat detection, information assurance, and resilience may be what keeps businesses safe while they make the most of innovative technology.

The overall IT perimeter for many enterprises and institutions is now more intricate and spread out because of on-premises systems, cloud computing, and edge computing. This means that threat detection, analysis, and incident response need to be better, and there has to be greater visibility. This element is an important part of smart cybersecurity. Smart cybersecurity can find, filter, neutralize, and fix cyber threats. It has a lot of potential.

AI tools for threat intelligence and network surveillance can help make cybersecurity better. Generative AI (GenAI) algorithms might use predictive models more effectively in cybersecurity, which would result in better security data and better outcomes. Gen AI might be able to apply predictive models in cybersecurity in a way that works better, giving better results and more trustworthy security data. AI agents and GenAI could work together to suggest ways to reduce risk and improve businesses and organizations' cybersecurity expertise and incident response. Generative AI can quickly find useful information, the best ways to do things, and proposed actions from the body of knowledge in the security business.

Also, Agentic AI-enabled cybersecurity has a lot of potential for finding, blocking, stopping, and fixing cyberthreats. Agentic AI can help with the main problems of threat detection, reaction speed, and analyst workload. These technologies automate tasks while still allowing human monitoring, which makes security teams work better in a more dangerous digital world.

With enhanced analysis of background information, practitioners can quickly figure out what kind of attack it is and what they should do next. This factor alone can shorten the time that bad actors spend on a site from days to just minutes, which is a significant plus for cyber defenders.

Smart algorithms can be applied to monitor the network for anomalous behavior, find new dangers that don't have visible signs, and take the right steps. It can also be used to compare data from different silos to figure out network risks and weaknesses, and the methods of attacks that are happening. Identity and access management are an important part of zero trust cybersecurity. AI could help by validating the accuracy of data across numerous remote databases.

To protect digital convergence, AI will need to be used in cybersecurity defenses and the development of next-generation cyber capabilities, such as predictive security and analytics. AI will be able to improve cybersecurity in areas like Data Loss Prevention (DLP), data privacy and identity governance, data access restrictions, risk assessment, and managing the security posture of data for data discovery and categorization.

Cybersecurity and AI are key areas of focus in the emerging digital ecosystem. These AI and computing technology tools can also contribute to advancements in various fields, including genetic engineering, augmented reality, robotics, renewable energies, big data, digital security, and quantum computing. Get ready for an innovative and exciting, but potentially precarious ride.

6. Quantinuum Overcomes Last Major Hurdle to Deliver Scalable Universal Fault-Tolerant Quantum Computers by 2029

by Simon Bisson
https://www.quantinuum.com/blog/quantinuum-overcomes-last-major-hurdle-to-deliver-scalable-universal-fault-tolerant-quantum-computers-by-2029

Quantum computing companies are poised to exceed $1 billion in revenues by the close of 2025, according to McKinsey & Company, underscoring how today's quantum computers are already delivering customer value in their current phase of development.

This figure is projected to reach upwards of $37 billion by 2030, rising in parallel with escalating demand, as well as with the scale of the machines and the complexity of problem sets of which they will be able to address.

Several systems on the market today are fault-tolerant by design, meaning they are capable of suppressing error-causing noise to yield reliable calculations. However, the full potential of quantum computing to tackle problems of true industrial relevance, in areas like medicine, energy, and finance, remains contingent on an architecture that supports a *fully fault-tolerant universal gate set with repeatable error correction*—a capability that, until now, has eluded the industry.

Quantinuum is the first—and only—company to achieve this critical technical breakthrough, universally recognized as the essential precursor to scalable, industrial-scale quantum computing. This milestone provides us with the most de-risked development roadmap in the industry and positions us to fulfill our promise to deliver our universal, fully fault-tolerant quantum computer, *Apollo*, by 2029.

In this regard, Quantinuum is the first company to step from the so-called "NISQ" (noisy intermediate-scale quantum) era towards utility-scale quantum computers.

Unpacking our achievement: first, a 'full' primer

A quantum computer uses operations called *gates* to process information in ways that even today's fastest supercomputers cannot. The industry typically refers to two types of gates for quantum computers:

- **Clifford gates**, which can be easily simulated by classical computers, and are relatively easy to implement; and
- **Non-Clifford gates**, which are usually harder to implement, but are required to enable true quantum computation (when combined with their siblings).

A system that can run both gates is classified as universal and has the machinery to tackle the widest range of problems. Without non-Clifford gates, a quantum computer is non-universal and restricted to smaller, easier sets of tasks - and it can always be simulated by classical computers. This is like painting with a full palette of primary colors, versus only having one or two to work with. Simply put, a quantum computer that cannot implement 'non-Clifford' gates is not really a quantum computer.

A fault-tolerant*,* or error-corrected, quantum computer detects and corrects its own errors (or faults) to produce reliable results. Quantinuum has the best and brightest scientists dedicated to keeping our systems' error rates the lowest in the world.

For a quantum computer to be *fully* fault-tolerant, *every operation* must be error-resilient, across Clifford gates *and* non-Clifford gates, and thus, performing "a full gate set" with error correction. While some groups have performed fully fault-tolerant gate sets in academic settings, these demonstrations were done with only a few qubits and error rates near 10%—too high for any practical use.

Today, we have published two papers that establish Quantinuum as the first company to develop a complete solution for a universal fully fault-tolerant quantum computer with repeatable error correction, and error rates low enough for real-world applications.

This is where the magic happens

The first paper describes how scientists at Quantinuum used our System Model H1-1 to perfect *magic state production*, a crucial technique for achieving a fully fault-tolerant universal gate set. In doing so, they set a record magic state infidelity (7×10^{-5}), 10x better than any previously published result.

Our simulations show that our system could reach a magic state infidelity of 10^{-10}, or about one error per 10 billion operations, on a larger-scale computer with our current physical error rate. We anticipate reaching 10^{-14}, or about one error per 100 trillion operations, as we continue to advance our hardware. This means that our roadmap is now derisked.

Setting a record magic state infidelity was just the beginning. The paper also presents the first break-even two-qubit non-Clifford gate, demonstrating a logical error rate below the physical one. In doing so, the team set another record for two-qubit non-Clifford gate infidelity (2×10^{-4}, almost 10x better than our physical error rate). Putting everything together, the team ran the first circuit that used a fully fault-tolerant universal gate set, a critical moment for our industry.

Flipping the switch

In the second paper, co-authored with researchers at the University of California at Davis, we demonstrated an important technique for universal fault-tolerance called "code switching".

Code switching describes switching between different error correcting codes. The team then used the technique to demonstrate the key ingredients for universal computation, this time using a code where we've previously demonstrated full error correction and the other ingredients for universality.

In the process, the team set a new record for magic states in a distance-3 error correcting code, over 10x better than the best previous attempt with error correction. Notably, this process only cost 28 qubits instead of hundreds. This completes, for the first time, the ingredient list for a universal gate setin a system that also has real-time and repeatable QEC.

Fully equipped for fault-tolerance

Innovations like those described in these two papers can reduce estimates for qubit requirements by an order of magnitude, or more, bringing powerful quantum applications within reach far sooner.

With all of the required pieces now, finally, in place, we are 'fully' equipped to become the first company to perform universal fully fault-tolerant computing—just in time for the arrival of Helios, our next generation system launching this year, and what is very likely to remain as the most powerful quantum computer on the market until the launch of its successor, Sol, arriving in 2027.

7. Bringing post-quantum cryptography to Windows

by Simon Bisson
https://www.infoworld.com/article/4012664/bringing-post-quantum-cryptography-to-windows.html

Microsoft prepares for security in a world where our old codes are easily broken. Get familiar with these technologies now before they become necessary.

Much of what we do to keep our online lives secure relies on public-key cryptography and its complex mathematical operations. At the heart of these techniques are sets of one-way functions that generate the public and private keys used to encrypt and decrypt data.

Those mathematical functions are secure because it would take immense amounts of time and computational power to find a private key from a public key, factor very large numbers, and then decrypt data — at least, if you're using a conventional computer. Some algorithms can be cracked using specialized hardware, but even here cost is still an issue.

Quantum computing and modern cryptography

One technology on the horizon could make the cryptographic basis of our entire online world obsolete almost overnight. Quantum computing uses low-temperature physics to build qubits, structures that can hold all the possible states, and then constructs quantum circuits that embody complex algorithms and quickly collapse probabilities to answer problems that would take many thousands of years with conventional computers.

Quantum computing factorization tools such as Schor's Algorithm require millions of qubits to factor a single public key, and today's quantum computers offer a mere handful of qubits. The technology that underpins quantum computing is advancing rapidly, with Microsoft and other companies developing new materials and error correction techniques to deliver stable qubits at scale and at an economically feasible cost.

That doesn't mean the entire world of computing will be upended overnight. The first at-scale quantum computers are still years away and are likely to initially be used for pure science. As they get easier and cheaper to build, they will be used by governments and by criminals looking to decrypt decades of financial data and other secrets.

Into the post-quantum world

For now we're safe. We have time to protect our secrets with new encryption algorithms designed to prevent quantum computing-based factorization. These post-quantum encryption algorithms take a symmetric approach to cryptography as opposed to the commonly used asymmetric algorithms that form the basis of much of today's public-key infrastructures.

The intent is to use new mathematical approaches that are hard for both conventional and quantum computers to solve. Of course, there are downsides: The keys are larger and need more processing time, compute capacity, and memory. For now, post-quantum cryptography is saved for valuable information where there's economic incentive for bad actors to use quantum computing to decrypt your data.

Part of the transition to post-quantum cryptography is the standardization of new algorithms and making them available in common cryptographic libraries, especially those used by both OS and applications. Microsoft has been working with the National Institute of Standards and Technology (NIST) to standardize these new algorithms and has begun adding them to its base SymCrypt library.

Adding post-quantum cryptography to Windows

Used across Microsoft's platforms, SymCrypt is a key component of tools such as Windows' Cryptographic Primitives Library and also offers support on Linux for use in Azure. It now supports the ML-KEM, ML-DSA, and SLH-DSA post-quantum cryptographic algorithms. The field is still evolving, and although you can use these algorithms now, better ones may come along in the future, so be ready to change if necessary.

ML-based algorithms use a Module Lattice (ML) approach, while SLH is a Stateless Hash. ML-KEM was originally known as Kyber and uses a mix of mathematical techniques to increase the complexity of the process used to generate a key pair. Module lattice techniques are based on what are called "lattice problems," which are hard to solve using computers. In fact, the hardest versions are so complex that even quantum computers will be challenged. It gets even more difficult when combined with an approach called "learning with errors" that adds noise to the process. This combination is why NIST has chosen ML-based algorithms for the FIPS-203 and 204 standards.

Preparing for the future, today

These algorithms are now available for Windows developers using Windows Insider builds as part of its Cryptography API Next-Generation libraries. This first release gives you access to ML-KEM for key encapsulation and ML-DSA for digital signatures. Using these now starts to protect you from what's known as "harvest now, decrypt later" attacks.

By keeping samples of encrypted data (especially key exchanges) to decrypt when quantum computers become usable, historic data that was secret will be easily recovered, opening trails of financial transactions or government messages that could still have relevant information. Microsoft suggests you mix these new algorithms with existing ones to give you deeper defenses.

You can use a less computationally intensive version of ML-KEM for now while you prepare for a complete shift to newer cryptographic systems and any necessary supporting hardware. It's likely that post-quantum cryptography will require a new generation of processor instructions or even dedicated accelerators to get the performance users and applications require.

Microsoft is adding support for post-quantum cryptography in its wincrypt tool, which provides APIs for the Windows certificate handling tools. You will be able to use ML-DSA certificates, managing them in the Windows certificate store and checking validity and trust.

Building post-quantum cryptography apps

At the heart of Microsoft's Windows implementation of post-quantum cryptography is what it calls "Cryptography API: Next Generation" (CNG). CNG is intended to replace the current Windows cryptography APIs, so it makes sense as the home for next-generation cryptosystems like ML-KEM and ML-DSA. It's a low-level library for use with C or C++. It's been in development for some time now and is mature enough to use as it offers a flexible set of features to support most common use cases.

Microsoft's CNG documentation recently added sample C++ code for working with both ML-DSA and ML-KEM. You can use familiar tools like Bcrypt to first load the post-quantum encryption algorithm you want to use from Microsoft's own implementation (though as always you have the option of using a third-party version).

Generating a key pair uses the same steps as traditional encryption, generating pairs and setting their properties. For example, with ML-DSA, this sets the parameter set that's being used. Choosing the right one is important, as this affects both the strength of the encryption method and its performance. As always this is a trade-off: The stronger the encryption, the longer it will take to create the key pair or a hash.

The process of generating a key or a hash with a post-quantum algorithm will be much the same as working with any other cryptographic algorithm today. Along with snippets of sample code, Microsoft provides complete modules you can use as the basis of any code you write.

Microsoft's Linux post-quantum tools

Microsoft isn't only delivering post-quantum cryptography in Windows, it's also using SymCrypt as a cryptography provider for OpenSSL on Linux. This is intended to provide FIPS certification, something that it needs for its Azure government cloud services. This is being used to test post-quantum-based Transport Layer Security (TLS) operations using hybrid key exchange.

This is only a first step to robust post-quantum cryptography across the Microsoft platform, as the necessary standards themselves are still in their infancy. More algorithms will be added, with support for Windows TLS as part of its TLS 1.3 implementation. It's also likely to be used sooner rather than later in Active Directory as part of its certificate services, generating ML-DSA-based certificates.

Microsoft is working on what it calls "crypto agility," the ability to swap out new algorithms as they develop, and is using hybrid techniques that mix current techniques with post-quantum cryptography to balance both resources and protection while support and algorithms mature.

Post-quantum cryptography isn't essential yet, but neither can you ignore it. It's a good idea to try out these new features and see how the new algorithms affect your applications. If certificates and signatures take longer to use and require more resources, it's important to understand how these latencies will impact your applications and whether you need to consider investing in new hardware now rather than waiting until the last minute.

8. Crypto Warning: NYDIG Flags Google's Quantum Jump as a Threat to Bitcoin Security

https://the420.in/bitcoin-quantum-computing-threat-security-cryptography-upgrade-needed/

A recent breakthrough in quantum computing by Google has reignited security concerns across the cryptocurrency world, especially regarding Bitcoin. In its latest development, Google's research team announced it had reduced the theoretical number of qubits needed to break RSA encryption—from 20 million to just 1 million. This development signals a dramatic acceleration in quantum computing capabilities, bringing once-distant fears much closer to reality.

While Bitcoin doesn't use RSA encryption, the shockwaves from this advancement extend to all digital security systems. The real question: could Bitcoin's own cryptographic foundations be next?

How Bitcoin's Security Could Be Impacted by Quantum Advancements

Bitcoin's cryptographic infrastructure relies on the Elliptic Curve Digital Signature Algorithm (ECDSA), and more recently, Schnorr signatures. These provide superior privacy, faster processing, and efficient multi-signature aggregation compared to older systems like RSA. However, despite these improvements, they are not immune to the power of a quantum computer.

The concern stems from Shor's Algorithm—a quantum algorithm developed in 1994 that can, in theory, break ECDSA and Schnorr-based cryptography if executed on a quantum machine with sufficient power. Currently, no such computer exists. But with quantum machines already exceeding 100 qubits and error correction technology rapidly maturing, the theoretical is inching toward the practical.

The **New York Digital Investment Group (NYDIG)** has warned that while Bitcoin is safe from today's quantum computers, it may not remain so a decade from now. The crypto community must understand that Bitcoin's long-term resilience is tied not just to hash rates and miners, but to advances in quantum-resistant encryption.

Can Post-Quantum Cryptography Secure Bitcoin?

To stay ahead of future threats, researchers and developers are working on Post-Quantum Cryptography (PQC)—new encryption methods designed specifically to withstand attacks from quantum computers. But integrating PQC into Bitcoin is no small task.

The NYDIG report outlines several obstacles:

- **Larger cryptographic keys and signatures**, which could bloat Bitcoin's blockchain
- **Slower transaction speeds**, undermining scalability
- **Potential compatibility issues** with existing wallet infrastructure and nodes

Moreover, Bitcoin's decentralized nature makes consensus around protocol upgrades especially complex and time-consuming. Still, the urgency for such changes is growing. The crypto industry may soon face a fork in the road: innovate or risk exposure to one of the biggest technological shifts of the century.

9. Fortanix launches PQC Central to assess cryptographic risk and exposure

by Duncan Riley
https://siliconangle.com/2025/06/25/fortanix-launches-pqc-central-assess-cryptographic-risk-exposure/

Multicloud security firm Fortanix Inc. today announced the launch of PQC Central, a new feature in its Key Insight tool that reframes how enterprises approach the post-quantum cryptography challenge.

The new feature seeks to address the security challenges that will arise with the emergence of quantum computing, which will threaten current cryptographic standards and demand proactive adaptation. Fortanix argues that organizations must act now to protect their data and infrastructure before quantum computing enters the mainstream.

PQC Central, which is embedded in Key Insight, helps organizations turn PQC migration complexity into actionable insights and strategic priorities. The service answers a critical question: How exposed are you? Before generating a prioritized list to guide PQC migration planning through Data Security Manager, the encryption and key management solution in Fortanix Armor, the company's enterprise-grade security platform.

The algorithms supported include Leighton-Micali Signature, Xtended Merkle Signature Scheme, Advanced Encryption Standard, Secure Hash Algorithm, CRYSTALS Kyber and CRYSTALS Dilithium.

With the announcement today, Fortanix Armor now offers end-to-end PQC readiness to help organizations navigate the shift to quantum-resistant encryption.

Fortanix Armor can now scan systems and services to discover cryptographic usage, map dependencies and catalog assets that rely on vulnerable algorithms, allowing enterprises to understand their exposure and to begin forming a comprehensive mitigation strategy.

The service assesses risk by identifying vulnerable keys and then generates a cryptographic readiness score to ensure that any systems reliant on outdated or at-risk encryption are flagged and prioritized for remediation. A centralized dashboard also allows security teams to track progress across environments and integrates with familiar information technology operations such as ServiceNow Inc. and Atlassian Corp.'s Jira to plan and manage the transition.

Fortanix Armor's crypto agility capabilities are also built to support evolving cryptographic standards, giving organizations the ability to adapt without modifying their existing key management systems or hardware security modules. Doing so supports long-term resilience by simplifying the implementation of updated algorithms or policies, ensuring continuous protection against future quantum threats, the company says.

"Post-quantum security may feel like tomorrow's problem, but protecting yourself today is a must to eliminate vulnerabilities and prevent future breaches," said Chief Product Officer Anuj Jaiswal. "PQC Central gives organizations the clarity and control they need to take action now and protect themselves from imminent disasters."

10. North Korean Hackers Try to Steal Crypto Via Deepfake Zoom Call

by J.R. Johnivan
https://www.techrepublic.com/article/news-north-korea-deepfake-zoom-crypto-attack/

North Korean hackers recently used deepfake technology in an attempt to impersonate executives from a cryptocurrency foundation, staging a convincing Zoom meeting to deceive an unsuspecting employee, according to cybersecurity firm Huntress.

Although it's unclear if their hack was successful, investigators believe the group's goal was to access and steal cryptocurrency linked to the victim's organization. The fact that their attack targeted a system running macOS only highlights the increasing sophistication of AI-driven attacks around the globe.

“Over the last few years, we have seen macOS become a larger target for threat actors, especially with regard to highly sophisticated, state-sponsored attackers,” a spokesperson for Huntress said in a recent interview.

Understanding how it happened

The breach reportedly began when the employee received an unnamed Calendly invitation for an upcoming meeting with company executives. However, the link redirected the user to a fake Zoom domain controlled by the attackers, Huntress said.

The second phase unfolded weeks later when the scheduled Zoom call took place. The employee joined the meeting and was greeted by what appeared to be members of the company’s leadership – their identities were later revealed to be deepfakes created by AI.

When the user encountered audio issues, they were encouraged to install a Zoom extension to fix the problem. In reality, the file was a malicious AppleScript designed to compromise macOS systems.

Huntress was made aware of the incident in June 2025. After dissecting the original AppleScript file, they found that it contained several malicious commands, remote codes, keyloggers, and backdoors. They also managed to trace the hack to a North Korean group known as TA444, aka BlueNoroff, Sapphire Sleet, COPERNICIUM, STARDUST CHOLLIMA, and CageyChamleon.

Once activated, the hack was designed to search the user’s hard drive for any accessible cryptocurrency wallets, which it would then attempt to hijack. The malicious program was also coded in a way to capture the contents of the user’s clipboard history and clean up after itself when it was done.

Avoiding similar attacks in the future

In their report covering the incident, Huntress provided useful recommendations on how users can avoid similar attacks in the future. Many of their recommendations are geared toward remote workers – as they’re the most likely to be targeted – but apply more broadly across hybrid work environments.

- Never trust a calendar invitation from someone you don’t know, someone you haven’t communicated with recently, or from people who don’t normally attend company meetings.

- Any sudden or unexpected changes, such as switching to another platform, installing extensions or plugins, visiting suspicious domain names, or allowing remote access to your device, should be taken as immediate red flags.

If you notice any of these indicators, disconnect from the meeting immediately and report the incident to your company’s HR or cybersecurity team.

Recognizing hacks, cyberattacks, and deepfakes before it’s too late

While this was a highly sophisticated and technical attack targeting an operating system that doesn’t see much malicious activity, there were several red flags during the multi-week ordeal that would have been concerning to any tech-savvy employee. When the legitimacy of a message or meeting requests is in question, it's best to contact a verified member of the organization through an alternate channel, preferable by phone, to confirm its authenticity. Taking this extra step can help prevent costly breaches and reputational harm.

11. QED-C® Report Recommends Ways to Strengthen Quantum Talent Pipeline and Fill Critical Quantum-Related Positions

https://quantumconsortium.org/qed-c-report-recommends-ways-to-strengthen-quantum-talent-pipeline-and-fill-critical-quantum-related-positions/

The Quantum Economic Development Consortium (QED-C) released a new report that looks at ways to strengthen the quantum industry's talent pipeline and bridge the gap between classroom formal education and hands-on experience required for quantum-related roles. QED-C's State of the Quantum Industry Report found that there are over 7,000 quantum jobs open globally today. Other recent data shows some 175,000-190,000 quantum jobs are projected in the Midwest U.S. alone by 2035.

Given the growing need in the quantum industry for skilled workers, QED-C convened a group of stakeholders to review some of the challenges and opportunities when it comes to filling the quantum talent pipeline. The report, called "Connecting the Dots: Quantum Learning Through Experiential Activities and Practice", noted that jobs will require people who can bridge technical and business domains, working in roles like engineers, technicians, and translators.

"Without a robust and skilled workforce, it will be impossible for the quantum ecosystem to live up to its full potential. That's why reports like this are so important, providing practical advice and a roadmap for organizations that will be critical to filling the quantum talent pipeline," said QED-C Executive Director Celia Merzbacher.

The report noted the quantum workforce currently faces numerous challenges, including:

- Educational systems that are falling short in providing practical training for quantum-related careers
- Lack of mentorship
- Unclear career paths
- Limited access to affordable, flexible training

The authors called experiential learning, or when skills are gained through experience rather than through the classroom, the "linchpin to integrate workforce readiness with the industry's rapid technological advances." They noted that programs like apprenticeships can help develop job-ready skills in lieu of traditional rote education.

The report also emphasized the need for early and continuous engagement on quantum technology and for more clarity, guidance, and mentorship for those considering a quantum career.

The report recommended the following actions to better create a bridge between industry and the educational institutions supplying quantum talent:

- Track and communicate current efforts in quantum workforce development, including establishing a central repository of efforts, opportunities, and outcomes
- Develop and deploy pilot programs that test scalable experiential learning models
- Coordinate ecosystem funding to monitor and identify opportunities to align public and private investments to strengthen workforce development

"Implementing these recommendations will make the road to a quantum career easier for more people. Our report makes clear that we must take action to bridge existing knowledge and skills gaps to fill critical roles in the quantum industry," said David Stewart, Executive Director of the Purdue Quantum Science and Engineering Institute and chair of the QED-C Workforce Technical Advisory Committee.

12. EU begins coordinated effort for Member States to switch critical infrastructure to quantum-resistant encryption by 2030

by Anna Ribeiro
https://industrialcyber.co/regulation-standards-and-compliance/eu-begins-coordinated-effort-for-member-states-to-switch-critical-infrastructure-to-quantum-resistant-encryption-by-2030/

The European Union is moving to strengthen its cybersecurity posture with the adoption of post-quantum cryptography. Backed by the European Commission, Member States have issued a roadmap and timeline to begin transitioning to this advanced form of encryption. The set of recommendations that Member States need to implement for a synchronised transition to post-quantum cryptography is divided into 'First Steps' that are required to initiate the transition, and 'Next Steps' that should follow.

Following the Commission's Recommendation issued last April, the EU move stems from a strategy developed by the NIS Cooperation Group and reflects growing urgency for Europe to act as quantum computing capabilities accelerate. Post-quantum cryptography is built on algorithms designed to resist decryption by quantum computers, marking a significant step toward defending against next-generation cyber threats. All EU Member States are expected to begin the shift by the end of 2026, with critical infrastructure required to complete the transition no later than 2030.

"As we enter the quantum era, post-quantum cryptography is essential to ensure a high level of cybersecurity, fortifying our systems against future threats," Henna Virkkunen, executive vice-president for technological sovereignty, security, and democracy, said in a media statement. "The post-quantum cryptography roadmap provides a clear direction to ensure the robust security of our digital infrastructure."

Titled *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, the document is the first deliverable from the NIS Cooperation Group's post-quantum cryptography work stream. It serves as an initial high-level guide for EU Member States. Many of the steps outlined for the post-quantum cryptography transition constitute 'no-regret' moves; they improve cybersecurity in general and support compliance with cybersecurity regulations, in particular the NIS2 Directive.

The roadmap recommends that Member States initiate a national post-quantum cryptography transition strategy following First Steps by the end of 2026 and coordinate their efforts at the EU level. At the same time, high-risk use cases should be transitioned to post-quantum cryptography as soon as possible, no later than the end of 2030. Furthermore, quantum-safe upgrades should then be enabled by default, and the post-quantum cryptography transition plans should be refined, in particular by implementing the recommended Next Steps.

By 2035, the transition should be completed for as many systems as practically feasible. This ambitious timeline is justified by the severe consequences broken cryptography would have on safeguarding data and securing sensitive communications, which are vital for the EU and its Member States' society, economy, security, and prosperity.

Last April, the European Commission initiated calls for proposals within Horizon Europe's 2023-2024 digital, industrial, and space work program, focusing on research and innovation in artificial intelligence (AI) and quantum technologies. With an investment of €112 million in AI, and quantum research and innovation, a new series of calls has been introduced, totaling over €112 million from the 2023-2024 Horizon Europe Digital, Industry, and Space work program.

The recommendations in this document include measures to ensure that stakeholders are informed of the quantum threat to cryptography and can exchange their knowledge and experience at the national, European, and international levels. It is recommended to ensure that the quantum threat becomes a part of the risk management of relevant entities and to establish mature cryptographic asset management to facilitate the transition to post-quantum cryptography and improve cryptographic agility in general.

As part of the 'First Steps,' the EU outlines eight foundational components for transitioning to post-quantum cryptography. One of the initial priorities is engaging key stakeholders early, including cybersecurity leaders, government agencies, and technical experts, to ensure coordinated planning and execution. This includes CTOs, CISOs, CIOs from critical sectors, government bodies, research institutions, and national cybersecurity authorities. Their coordinated input is essential for shaping and executing a national roadmap.

Organizations must also improve cryptographic asset management by keeping detailed and current inventories of all systems using cryptography. These should be supported by asset management tools and standards such as cryptographic bills of materials. Accurate inventories are vital for effective risk management and business continuity planning.

It is also necessary to map internal and external dependencies across applications, platforms, and operational processes. Understanding these connections enables smoother migration planning, better supply chain coordination, and interoperability across the EU.

Quantum-related threats should be integrated into national and organizational risk assessments. These risks must be elevated to board-level discussions and reflected in public cybersecurity reports to ensure adequate attention and resources.

The supply chain must be engaged early in the process. Product and service providers need to align their roadmaps with post-quantum cryptography goals and ensure cryptographic agility is built into their offerings. This coordination supports both national and EU-level transition strategies.

Raising awareness across organizations is also essential. Targeted, role-specific programs should be developed to educate personnel about quantum threats and cryptographic transition priorities. Multiple communication channels, including official platforms, social media, and industry publications, should be used to deliver timely and accurate information.

Knowledge sharing and collaboration should be prioritized through participation in expert communities, international dialogues, and the NIS Cooperation Group's work stream on post-quantum cryptography. This helps synchronize efforts across borders and sectors.

Finally, each country should establish a national timeline and implementation plan. Priorities should be clearly defined using a flexible prepare-plan-act framework. Timelines will vary depending on specific use cases, but a coordinated and adaptable strategy will support a more secure and resilient transition. These initial actions are critical to building a unified and well-informed path toward quantum-resistant cryptographic systems across the EU and its member states.

After work on the First Steps has started and an initial implementation plan has been established, it is important to pursue activities that could help to carry out a smooth migration and to fine-tune and update the implementation plan continuously. Further actions which should be considered in this process.

As part of its 'Next Steps,' the EU emphasizes the need to build cryptographic agility and prepare a secure upgrade path for future systems. New products must be designed with the flexibility to update cryptographic mechanisms as threats evolve. Beginning in December 2027, this will be a formal requirement under the Cyber Resilience Act. Even before full transition to post-quantum cryptography, products should be capable of receiving software and firmware updates signed with quantum-safe algorithms. Update mechanisms must be in place, using standardized post-quantum signatures, and procurement processes should explicitly require this level of agility.

Ongoing engagement with stakeholders and vendors is essential to refine migration strategies and maintain alignment across industry and regulation, including compliance with evolving frameworks like NIS2. The EU calls for allocating the necessary budget and skilled personnel to manage the complexity of this transition. Lifecycle management costs must be factored in from the outset to ensure continuity.

Certification schemes must also be adapted. National and European cybersecurity certification systems under the Cybersecurity Act need to reflect quantum-era threats. Collaboration with groups such as the EU Cybersecurity Certification Group is encouraged to ensure up-to-date guidance. These requirements must be embedded into product evaluations, procurement protocols, and regulatory compliance, with close coordination among NIS2 and eIDAS supervisory bodies.

The regulatory landscape requires review and revision. Existing national laws related to cryptography should be updated to incorporate post-quantum standards. Where such laws do not exist, new frameworks must be developed. These updates should be informed by input from peer countries and the NIS Cooperation Group. Post-quantum cryptography requirements should start to appear in procurement contracts, certifications, and partnership agreements.

The EU sees strong potential in leveraging its cybersecurity ecosystem. Public-private partnerships are needed to help vendors and service providers align with national migration roadmaps. Training programs must be updated or created to equip cybersecurity professionals and specialists with post-quantum cryptography knowledge. Member States are urged to pool educational resources and share experiences to accelerate capacity building. Funding opportunities, both national and European, should be directed toward post-quantum cryptography implementation. Cyber coordination centers and competence hubs can support these efforts.

International cooperation plays a central role. The EU should actively participate in global post-quantum cryptography standardization work and promote collaboration between national and EU initiatives. Authorities are encouraged to support research, share technical knowledge, and build joint programs, including PhD-level study and innovation.

Pilots and testing infrastructure must also be developed and expanded. Engagement in international testbeds, such as ETSI Plugtests and IETF post-quantum cryptography hackathons, will provide valuable insights. National centers of expertise can further enhance readiness. Real-world use cases should guide the testing phase to ensure that any deployment is grounded in operational resilience and threat reality. This multi-layered approach reflects the EU's commitment to a secure and coordinated shift to post-quantum cryptography, ensuring systems remain trusted and resilient in a quantum-capable future.

In May, the Post-Quantum Cryptography Coalition (PQCC) released its Post-Quantum Cryptography Migration Roadmap to assist organizations in navigating the complexities of transitioning to quantum-safe cryptography. The comprehensive and tailorable guide provides a strategic framework across four critical categories – preparation, baseline understanding, planning and execution, and monitoring and evaluation, equipping organizations with actionable tools and methodologies to safeguard their data against emerging quantum threats.

13. China breaks RSA encryption with a quantum computer, threatening global data security

by Eric Ralls
https://www.earth.com/news/china-breaks-rsa-encryption-with-a-quantum-computer-threatening-global-data-security/

If you logged onto your bank account this morning, the security protocols still seem secure – but things are changing quickly in the tech world. A team in China just showed that the math behind RSA encryption is starting to bend to the will of the quantum realm.

Using a quantum annealing processor built by D-Wave Systems, the researchers say they factored a 22-bit RSA integer that had resisted earlier attempts on the same class of hardware. Wang Chao and colleagues at Shanghai University carried out the experiment.

RSA's reputation for toughness

When RSA encryption debuted in 1977 it was lauded for tying security to the difficulty of splitting a large semiprime into its two prime factors .

Classic computers still need sub-exponential time to break today's 2048-bit keys, and the largest key so far cracked with conventional methods is only 829 bits (RSA-250) after weeks on a supercomputer.

"Using the D-Wave Advantage, we successfully factored a 22-bit RSA integer, demonstrating the potential for quantum machines to tackle cryptographic problems," the authors wrote.

The group translated factorization into a Quadratic Unconstrained Binary Optimization problem, which the D-Wave Advantage system solves by letting qubits tunnel through energy barriers seeking the lowest energy state.

They also applied the same method to Substitution–Permutation Network ciphers such as Present and Rectangle, calling it "the first time that a real quantum computer has posed a substantial threat to multiple full-scale SPN structured algorithms in use today."

Twenty-two bits still matter

A 22-bit key is trivially small compared with production-grade RSA, yet the test matters because the approach scaled beyond past demonstrations that stopped at 19- bits and required more qubits per variable.

Reducing the local-field and coupling coefficients in the Ising model cut noise, letting the annealer reach correct factors more often and hinting at paths to bigger keys, according to the paper.

"The advancement of quantum computers can seriously threaten data security and privacy for various enterprises," warned Prabhjyot Kaur of analyst firm Everest Group, who was not involved in the study.

Annealing vs. Shor's promise

Universal, gate-based quantum machines run Shor's algorithm, which in principle can shred RSA by finding the period of modular exponentiation in polynomial time.

Those devices still struggle with error correction, while D-Wave's annealers, though not universal, already pack more than 5000 qubits and avoid deep circuits by using a chilling 15 mK environment and analog evolution.

Annealing excels at combinatorial optimization, so the Shanghai team reframed factoring as that type of search problem instead of using Shor's period-finding route.

The strategy sidesteps current qubit-count limits of gate machines but pays a price in exponential scaling, which is why only a 22-bit modulus fell this time.

The policy clock keeps ticking

Standards bodies are not waiting. In August 2024 NIST released FIPS 203, 204 and 205, the first federal standards for post-quantum cryptography based on lattice problems, and in March 2025 it selected HQC for the next wave.

A White House event framing the publication urged U.S. agencies to begin swapping vulnerable keys because adversaries may already be hoarding encrypted data for "hack now, decrypt later" attacks.

"Businesses must treat cryptographic renewal like a multi-year infrastructure project," the Wall Street Journal's CIO briefing noted when the final standards neared release last year. Corporate technology leaders echoed that sense of urgency.

RSA vs. quantum cracking

Most businesses haven't yet updated their cryptography inventories, and many don't even know which algorithms their systems depend on.

Security experts recommend starting with an internal audit to identify all uses of RSA, ECC, and other vulnerable algorithms before building a replacement plan.

While full migration may take years, organizations can begin by testing quantum-safe libraries such as Open Quantum Safe, deploying hybrid key exchange methods.

Integrating crypto-agility – the ability to swap cryptographic algorithms without reengineering entire systems – is also a good option. This makes future upgrades less painful as new standards arrive.

What comes next and what to watch

Large-key RSA is still safe today, yet the study shows that hardware improvements and smarter embeddings keep shaving away at the gap.

D-Wave plans a Zephyr-topology processor with more than 7000 qubits later this year, and each topology upgrade improves connectivity, which in turn reduces the number of physical qubits needed per logical variable.

Cryptographers, meanwhile, recommend adopting hybrid schemes that wrap lattice-based algorithms such as CRYSTALS-Kyber around classical RSA signatures to provide forward secrecy during the transition period.

Organizations holding sensitive data for decades, health records, genomic files, diplomatic cables, have the most to lose if they wait until a full-scale quantum computer arrives.

Some observers point out that the Shanghai result relied on heavy classical pre- and post-processing, and that the annealer still required many runs to locate the right factors.

Even so, history shows that cryptanalytic proofs of concept rarely stay small: DES fell to a $250,000 machine in 1998 only four years after the first partial cracks surfaced.

14. “IBM Should Be Worried”: China Fires up 1,000-Qubit Quantum Computer and Sparks Panic in Global Supercomputing Race

by Eirwen Williams
https://www.rudebaguette.com/en/2025/06/ibm-should-be-worried-china-fires-up-1000-qubit-quantum-computer-and-sparks-panic-in-global-supercomputing-race/

In the rapidly evolving landscape of quantum computing, China has taken a significant leap forward with its latest innovation, the ez-Q Engine 2.0. This breakthrough represents a pivotal moment in the global quantum race, marking China’s emergence as a formidable contender. The system is designed to support quantum computers with over 1,000 qubits, positioning China just behind IBM and Atom Computing in terms of operational quantum systems. As the quest for quantum supremacy intensifies, China’s advancements in quantum technology not only challenge existing global leaders but also underscore the country’s commitment to becoming a dominant force in this revolutionary field.

China’s 1,000 Qubits Quantum Computing

China’s latest foray into quantum computing, the ez-Q Engine 2.0, is a groundbreaking system delivered to prestigious research institutions, including the University of Science and Technology of China and China Telecom Quantum Group. This revolutionary system is set to provide over 5,000 qubits of control services, marking a substantial increase in China’s quantum capabilities. Developed in Hefei, Anhui Province, the heart of China’s national quantum program, this system has been tested on the country’s 504-qubit superconducting quantum computer, setting new benchmarks for stability, signal fidelity, and system integration.

The ez-Q Engine 2.0 is hailed as a generational leap from its predecessor, the Zuchongzhi 3.0, which was a 105-qubit processor that claimed quantum computational advantage over traditional supercomputers. By integrating Chinese components, the system reduces physical footprints and operational costs significantly, offering a more efficient and cost-effective solution compared to foreign counterparts. This advancement highlights China’s commitment to developing indigenous technology and reducing reliance on foreign innovations.

Challenging US Quantum Leadership

The introduction of the ez-Q Engine 2.0 represents a direct challenge to US quantum leadership. This cutting-edge system has overcome technical hurdles in RF direct sampling and clock synchronization, achieving low-noise, high-precision signal handling, a feat previously dominated by US and European systems. IBM’s Condor chip, unveiled in late 2023, was the first superconducting quantum processor to surpass the 1,000-qubit threshold, featuring 1,121 qubits within its Quantum System Two architecture. Atom Computing followed closely, introducing a 1,125-qubit neutral atom-based system, currently holding the record for qubit count.

China’s platform, if independently validated, could rank as the third largest globally. QuantumCTek’s deputy director, Wang Zhehui, confirmed that the firm is already developing a control system for 10,000-qubit scale quantum processors. This system includes embedded error correction capabilities, essential for achieving quantum advantage in real-world applications. This development signifies China's strategic move towards building a self-reliant, industrial-grade quantum ecosystem, moving beyond mere replication of Western technology to competing in core infrastructure design.

The Broader Implications of China's Quantum Leap

The introduction of the ez-Q Engine 2.0 is not just an incremental step in China's technological journey; it represents a strategic shift in the global quantum race. While IBM and Atom Computing currently lead in raw qubit counts, China's new system, with its domestic design, cost efficiency, and control precision, narrows the technological gap. As quantum systems transition from demonstration to deployment, China's entry with what may be the world's third most capable quantum control platform signals a strategic shift in the global power dynamics of technology.

The era of quantum sovereignty is here, and the competition among nations is accelerating. China's advancements in quantum technology align with similar efforts in the US, where quantum systems are being integrated into national defense, AI acceleration, and cryptographic resilience. This development highlights China's commitment to becoming a leader in quantum technologies, matching its strategic rhetoric with tangible hardware delivery, and positioning itself as a formidable player in the global quantum landscape.

Looking Ahead: The Future of Quantum Computing

As China makes significant strides in quantum technology, the global landscape of computing is poised for dramatic transformations. The ez-Q Engine 2.0 is just the beginning of China's ambitious plans to revolutionize quantum computing. With continued investments in research and development, China aims to further solidify its position in the quantum realm, challenging the dominance of established players like IBM and Atom Computing. As these technologies continue to evolve, the implications for industries ranging from cryptography to artificial intelligence are profound.

As the competition in quantum computing heats up, the question remains: How will these advancements shape the future of technology, and what role will China play in this unfolding narrative of innovation and discovery?

15. QNu Labs Launches QNu Academy to Support National Quantum Mission

by TimesTech
https://timestech.in/qnu-labs-launches-qnu-academy-to-support-national-quantum-mission/

QNu Labs, India's first and world's no. 1 integrated end-to-end quantum secured cybersecurity platform announced the launch of QNu Academy, a global educational initiative aimed at building a future-ready talent pipeline in quantum technologies and cybersecurity. As India advances its digital infrastructure and aligns with the National Quantum Mission, QNu Academy, backed by National Quantum Mission aims to bridge the existing talent gap. This launch marks a strategic milestone in India's journey toward achieving quantum self-reliance and digital sovereignty.

QNu Academy offers in-depth education and practical training in advanced technologies such as Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG), and Post-Quantum Cryptography (PQC). The curriculum blends self-paced learning and instructor-led modules, curated in collaboration with experts from premier Indian institutions like the IITs and DRDO, as well as global quantum research bodies. Learners benefit from real-world use cases, hands-on lab assignments, continuous assessments, and mentorship from industry practitioners.

The academy is designed to serve a wide range of learners, including universities, faculties, and students, to build a skilled workforce capable of securing India's digital future. In addition, QNu Academy actively supports educational institutions through Faculty Development Programs and the creation of Centres of Excellence (CoE) Labs to promote quantum innovation and applied research. Placement support, certifications, and career readiness initiatives are also integrated into the learning journey.

Speaking on the launch, Sunil Gupta, Co-founder and CEO of QNu Labs, said, "QNu Academy is more than an educational platform. It is a national mission to democratize access to quantum education and build widespread awareness around quantum communications. Our goal is to create a sustainable ecosystem for quantum learning in India through faculty development programs, industry-relevant programs, CoE labs, certified programs, real-time projects, and assignments with placement opportunities to develop quantum experts, empowering you to become a future leader. The future of cybersecurity in India depends on how well we prepare today's learners to tackle tomorrow's threats."

"Through QNu Academy, we hope to foster a culture of innovation, encourage indigenous R&D in quantum tech, and empower India's workforce to lead on the global stage," he added.

QNu Academy represents a timely and important investment in human capital. The program aligns well with India's broader goals of technological development, digital resilience, and global leadership in quantum innovation. It is envisioned as a long-term commitment to enabling India's readiness for quantum disruption and equipping the country with the skilled manpower needed to thrive in the post-quantum era.

16. Internet users advised to change passwords after 16bn logins exposed

by Dan Milmo
https://www.theguardian.com/technology/2025/jun/21/internet-users-advised-to-change-passwords-after-16bn-logins-exposed

Internet users have been told to change their passwords and upgrade their digital security after researchers claimed to have revealed the scale of sensitive information – 16bn login records – potentially available to cybercriminals.

Researchers at Cybernews, an online tech publication, said they had found 30 datasets stuffed with credentials harvested from malicious software known as "infostealers" and leaks.

The researchers said the datasets were exposed "only briefly" but amounted to 16bn login records, with an unspecified number of overlapping records – meaning it is difficult to say definitively how many accounts or people have been exposed.

Cybernews said the credentials could open access to services including Facebook, Apple and Google – although there had been no "centralised data breach" at those companies.

Bob Diachenko, the Ukrainian cybersecurity specialist behind the research, said the datasets had become temporarily available after being poorly stored on remote servers – before being removed again. Diachenko said he was able to download the files and would aim to contact individuals and companies that had been exposed.

"It will take some time of course because it is an enormous amount of data," he said.

However, other cybersecurity experts said the data was likely to have already been in circulation and contain multiple repetitions.

One expert, speaking on condition of anonymity, said: "We're sceptical of the data, particularly how much of it is just repetition of the same information. It's difficult to verify it without having the data."

Diachenko said the information he had seen in infostealer logs included login URLs to Apple, Facebook and Google login pages. Apple and Facebook's parent, Meta, have been contacted for comment.

A Google spokesperson said the data reported by Cybernews did not stem from a Google data breach – and recommended people use tools such as Google's password manager to protect their accounts.

Internet users are also able to check if their email has been compromised in a data breach by using the website haveibeenpwned.com. Cybernews said the information seen in the datasets followed a "clear structure: URL, followed by login details and a password".

Diachenko said the data appeared to be "85% infostealers" and about 15% from historical data breaches such as a leak suffered by LinkedIn.

Experts said the research underlined the need to update passwords regularly and adopt tough security measures such as multifactor authentication – or combining a password with another form of verification such as a code texted from a phone. Other recommended measures include passkeys, a password-free method championed by Google and Facebook's owner, Meta.

"While you'd be right to be startled at the huge volume of data exposed in this leak it's important to note that there is no new threat here: this data will have already likely have been in circulation," said Peter Mackenzie, the director of incident response and readiness at the cybersecurity firm Sophos.

Mackenzie said the research underlined the scale of data that can be accessed by online criminals.

"What we are understanding is the depth of information available to cybercriminals."

He added: “It is an important reminder to everyone to take proactive steps to update passwords, use a password manager and employ multifactor authentication to avoid credential issues in the future.”

Toby Lewis, the global head of threat analysis at the cybersecurity firm Darktrace, said the data flagged in the research is hard to verify but infostealers – the malware reportedly behind the data theft – are “very much real and in use by bad actors”.

He said: “They don’t access a user’s account but instead scrape information from their browser cookies and metadata. If you’re following good practice of using password managers, turning on two-factor authentication and checking suspicious logins, this isn’t something you should be greatly worried about.”

Cybernews said none of the datasets have been reported previously barring one revealed in May with 184m records. It described the datasets as a “blueprint for mass exploitation” including “account takeover, identity theft, and highly targeted phishing”.

The researchers added: “The only silver lining here is that all of the datasets were exposed only briefly: long enough for researchers to uncover them, but not long enough to find who was controlling vast amounts of data.”

Alan Woodward, a professor of cybersecurity at Surrey University, said the news was a reminder to carry out “password spring cleaning”. He added: “The fact that everything seems to be breached eventually is why there is such a big push for zero trust security measures.”

17. Infineon discusses preparing for post-quantum cryptography

by Caitlin Gittins
https://www.iotinsider.com/industries/security/infineon-discusses-preparing-for-post-quantum-cryptography/

Infineon’s wholehearted embrace of post-quantum cryptography (PQC) and securing its solutions accordingly comes from its recognition of the threats that could be posed by quantum computing. Robert Bach, Product Marketing for Semiconductors ID Solutions at the company spoke to IoT Insider about its approach to PQC.

The company demonstrated how it is securing its products with the certification of one of its security controllers in January 2025. The solution in question was certified by the German Federal Office for Information Security and signified how it was preparing itself for quantum computers.

Quantum computers have the potential to crack conventional algorithms with their advanced computational capabilities and therefore must be considered in the development of products which have life cycles of 10 years and onwards.

“We’re talking about a device that has restricted resources,” explained Bach, referencing the security controller. “If you have a big computer [or] a big mainframe you can do all kinds of cryptography, you don’t have to reflect ‘is my hardware powerful enough?’

“But if you have a tiny security controller which should not be too expensive, inside of a smart card or an authentication product, you cannot, for example, double the functionality of that chip.”

This meant that the security controller was an especially challenging application to have PQC certified, and it still needed to be secured against classical attacks as well.

“That’s the reason why certification is so important, because with certification … you can have a very good feeling that the implementation has been done in a secure way,” added Bach.

Post-quantum cryptography journey

Infineon began its journey with PQC around a decade ago, when it implemented a PQC algorithm onto a contactless security chip. It won two SESAME Awards for its efforts.

“We intensified our approach to post-quantum cryptography three or four years ago,” explained Bach, “going out, telling everybody in the industry: please start preparing for the quantum computer and for quantum resilience.”

Preparedness across industries varies widely. Governmental institutions have been aware of the subject, Bach noted, but for some people there remain question marks about what quantum computing is and what to prepare for – drawing on an example of a speech that was given to German industry companies at an event last year, Bach said when he asked about who had heard of a quantum computer, around 10% of the audience raised their hands.

“There are industry segments where the awareness level still is very low,” Bach continued.

Companies like Zoom have already integrated PQC, however this has been a relatively simple application where integration is concerned. Applications like national ID cards and security controllers are trickier.

In terms of engaging with these industries that are less prepared and aware, Bach said at Infineon their approach was first to do their own “homework” as a semiconductor company before looking at other companies.

“What we’re saying is we do not know when the quantum computer will really come,” said Bach. “But what we would advise to our customers [is] you can already start now [with] using the hardware and start implementing.”

PQC in digital IDs

From his position, Bach addresses post-quantum cryptography from the perspective of government institutions involved in managing digital identities.

“What becomes very clear at least in a couple of countries [is that] a lot of governmental documents will be migrated soon to post-quantum cryptography. Because here you have the problem … that … once you put it out in the field, it stays in the field for 10 years.”

This time period is even longer for the automotive industry, where a security controller in a vehicle needs to be quantum secure for approximately 15-20 years.

The challenges aren't technical, said Bach, but are related to application standards, or the lack thereof: "Depending on the industry and the application … you need to have worldwide interoperability, otherwise you cannot travel."

This means that if one nation, for example France, decides to integrate PQC into its passport and Germany does not recognise this, a traveller wouldn't be able to cross over the border.

"First there must be an application standard," Bach stressed. "It is easier in closed systems, for example, for a car manufacturer. A car manufacturer can decide to migrate its cars early to quantum resilience, because they control the system … and they don't need … interoperability."

Therefore, implementation of PQC in digital identities is going to take longer because the standards first need to be agreed upon. This was why Infineon "started communicating years ago," said Bach, and discussions in governments about IDs are ongoing.

"You have two possibilities to mitigate [the effects]. First, you could think of reducing the lifetime of the documents. Instead of 10 years, you give out a passport for five years.

"The second topic, and that's discussed more and more, is to make the products upgradable in the field."

When I pointed out that some people may not be enamoured with having their passports issued every five years, instead of 10, Bach agreed; making the suggested upgradable route more attractive.

What does this look like?

"If you don't have an application standard, then your product, your ID card, has to fulfil the old application standard, otherwise you wouldn't be interoperable. Once a new standard comes in you have a possibility to upgrade via software products [in] the field."

Whether this is a digital identity, an IoT product or a vehicle, it means all of these solutions would be quantum secure and interoperable. These discussions around mitigations are ongoing, and no government has decided on what to do yet.

Future PQC roadmap

The certified security controller represents the first step for Infineon, who have plans to upgrade around 80% of its security controller portfolio to PQC, as well as integration into its standard microcontrollers and automotive controllers.

"Post-quantum cryptography is not really rocket science, [but] quantum computers might be," said Bach. "Quantum computers are complex …. Using post-quantum cryptography will get easier and easier, especially if you have all the products available.

"But we expect long transition periods because it is complex to upgrade the whole system to a new kind of cryptography. And this is valid for all kinds of industries."

Interestingly, Infineon is involved in working on components for quantum computers. In September 2024, it was awarded a contract along with Oxford Ionics to build a mobile quantum computer.

However, this shows that quantum computing as a technology isn't mutually exclusive: it doesn't only have to be viewed through the lens of security risks and therefore must be feared. It can also be leveraged as an invaluable tool for solving advanced computations and benefiting a wide array of industries.

"On one hand, we're fighting against quantum computers. On the other hand, it's not just necessary to concentrate on the bad things you can do with it. You can do a lot of good … with a quantum computer," Bach concluded.

18. Indian Army Secures Cyber Defence with Post-Quantum Cryptography

by Itishree Sethy
https://pragativadi.com/indian-army-secures-cyber-defence-with-post-quantum-cryptography/

The Indian Army has embraced indigenous Post-Quantum Cryptography (PQC) applications, designed and developed by the Military College of Telecommunication Engineering (MCTE) in Mhow, under the Corps of Signals.

The rollout of these advanced cryptographic solutions marks a watershed moment in India's defence technology roadmap.

These PQC tools aim to future-proof Army communication systems against the looming threat of quantum-enabled cyberattacks. As global security paradigms shift, traditional encryption methods face obsolescence in the face of rapidly advancing quantum computing. The Indian Army's proactive response—rooted in the Technology Research vision of the Chief of the Army Staff (COAS)—underscores its commitment to building a future-ready, digitally secure force.

Post-Quantum Cryptography algorithms rely on mathematics that remains resistant even to quantum attacks, thereby ensuring the confidentiality and integrity of classified military communications. With progressive integration into defence infrastructure, the initiative reaffirms India's commitment to self-reliant innovation under *Aatmanirbhar Bharat*.

This technological leap reinforces India's position as a forward-thinking military power, adapting to the digital age not only through weaponry but through resilient communication frameworks that will define the battlespace of tomorrow.

19. Q-Day Revisited – RSA-2048 Broken by 2030: Detailed Analysis

by Marin Ivezic
https://postquantum.com/post-quantum/q-day-y2q-rsa-broken-2030/

Introduction

It's time to mark a controversial date on the calendar: 2030 is the year RSA-2048 will be broken by a quantum computer. That's my bold prediction, and I don't make it lightly. In cybersecurity circles, the countdown to "Q-Day" or Y2Q (the day a cryptographically relevant quantum computer cracks our public-key encryption) has been a topic of intense debate. Lately, the noise has become deafening: some doom-and-gloom reports insist the quantum cryptopocalypse is just a year or two away, or is already here in secret government labs, while hardened skeptics claim it's so distant as to never happen. The truth lies between these extremes. A sober analysis of the latest breakthroughs shows that Q-Day is not here yet and won't happen tomorrow – but it's also no longer on the hazy horizon of "maybe never." In fact, recent advances have dramatically sharpened the timeline, bringing the fall of RSA into the plausible timeframe of around 2030.

As someone who's been tracking quantum computing progress and making public Q-Day predictions for over 15 years, I've consistently argued that it's not enough to watch the raw count of qubits in labs. We must also scrutinize improvements in quantum error correction, algorithm design, and the number of logical (error-corrected) qubits needed for an attack. Every few years I've updated my forecast accordingly. (Last one here: "*Q-Day Predictions: Anticipating the Arrival of CRQC*"). For years I held to an estimate of 2032 for Q-Day – but a string of major developments in just the last few days has compelled me to move that prediction forward.

Three pieces of recent news triggered this reassessment, each hitting a different "axis" of quantum progress: algorithmic efficiency, hardware error rates, and engineering roadmaps.

Here's the quick-and-dirty takeaway for the impatient and those that follow quantum computing news:

1. *IBM's latest roadmap (unveiled June 2025) targets a fault-tolerant system with ≈200 logical qubits by 2029 and clearly spells out a path to ≈1,000+ logical qubits by the early 2030s.*

2. *Gidney's May 2025 paper shows that ~1,000–1,400 logical qubits, running for about a week, are enough to factor RSA-2048 when paired with modern error-correction tricks.*

3. *~~Oxford's new fidelity record~~ (single-qubit gate error ≈ 1 × 10-7) hints that each logical qubit could soon be built from hundreds, not thousands, of physical qubits.*

Put those three facts together and my old 2032 Q-Day estimate is essentially baked in even if the field made zero further scientific breakthroughs after June 2025 and simply executed on what has just been published.

Realistically, though, we'll keep squeezing qubit overhead with better error-correction codes, smarter factoring circuits, and faster hardware integration. That steady drumbeat of incremental wins makes 2030 the likelier arrival date, and slipping past 2032 now feels like a long shot, not the baseline.

I unpack all the supporting data, caveats, and counter-arguments in the full article.

As I summarized, in just the past few weeks, researchers have slashed (physical) qubit requirements for factoring RSA-2048 from millions to under one million, demonstrated quantum gate fidelities at or beyond the threshold needed for effective error correction, and laid hardware roadmaps for large-scale fault-tolerant quantum computers by the end of this decade. In short, the pieces needed to factor a 2048-bit RSA key are rapidly falling into place. While this doesn't mean an overnight collapse of cryptography, it does mean governments and industry must urgently recalibrate their post-quantum migration plans. The three recent breakthroughs I analyzed in separate posts:

1. First, a new factoring algorithm published by Google researchers slashed the qubit count needed to factor RSA-2048 by an order of magnitude which I analyzed here: "*Quantum Breakthrough Slashes Qubit Needs for RSA-2048 Factoring*."

2. Second, physicists at Oxford achieved a record-breaking low error rate in quantum operations (only 1 error in 6.7 million), foreshadowing much lower overhead for error correction. I summarize their paper here: "*Oxford Achieves 10^{-7}-Level Qubit Gate Error, Shattering Quantum Fidelity Records*."

3. And third, IBM unveiled a detailed roadmap promising a fault-tolerant quantum computer by 2029 – years ahead of many expectations. I analyzed this announcement here: "*IBM's Roadmap to Large-Scale Fault-Tolerant Quantum Computing (FTQC) by 2029 – News & Analysis*."

These advances, in algorithmics, error correction, and scalable hardware, all point to the same conclusion: the timeline to a cryptoanalytically (or cryptographically) relevant quantum computer (CRQC) is accelerating.

The punchline? If current trends hold, a quantum computer capable of breaking RSA-2048 will likely exist by around 2030. That doesn't mean internet encryption collapses overnight or that we should all panic. But it does mean the prudent window for migrating to quantum-safe cryptography is right now. The latest science has shifted Q-Day from an "if" to a concrete question of "when," and the smart bet is "sooner than previously thought." Let's explore why.

.

.

.

From Weeks of Computation to Megawatts of Power: The Realities of an RSA-Breaking Quantum Computer

While I'll keep repeating that we should start preparing for Q-Day now, I also don't want to cause panic. Somewhat good news for cybersecurity professionals is that even once a cryptographically relevant quantum computer (CRQC) exists, breaking RSA-2048 won't be trivial in practice – it will likely be an expensive, specialized endeavor. Gidney's design, for instance, would consume on the order of a week of runtime on a million-qubit machine. Each 2048-bit number factored might require billions of quantum gate operations executed in sequence. In today's terms, that's a massive computation – by comparison, current noisy devices struggle to maintain state beyond a few hundred gates. So while a future CRQC could crack a single RSA key in, say, 3–7 days, it won't be cracking thousands of keys on a whim without significant upgrades in throughput.

Furthermore, the energy cost of such a feat will be enormous. Large-scale quantum computers (especially superconducting ones) demand power-hungry cryogenics and control systems. In my previous post "*The Enormous Energy Cost of Breaking RSA-2048 with Quantum Computers*" I tried to summarize why factoring a single RSA-2048 key could cost tens of thousands of dollars in electricity alone. Even with hardware improvements, we are likely talking tens of megawatt-hours of energy and many thousands of dollars in electricity per RSA key broken. (By contrast, classical supercomputers, while also power-hungry, would need billions of years to do the same task, so we've traded impossible time for heavy energy.) The takeaway is that early quantum attacks will be the domain of nation-states or elite organizations – those who can allocate dedicated facilities and power budgets to target the "crown jewels" of encrypted data. As I previously wrote "*not just about qubits and math; it's about megawatts*" as well.

From Forecast to Reality: Why I'm Predicting 2030 for Q-Day

Bringing together all these threads, let's answer the key question: When will RSA-2048 actually be broken by a quantum computer? My updated prediction, based on the evidence discussed, is 2030 – give or take a year. This is more aggressive than many past estimates, so let me clarify the reasoning and also what this implies for action.

First, consider the trendline. As the Google team noted, the resource estimates for quantum factoring have been dropping by roughly an order of magnitude every few years. In 2012: 10^9 qubits. In 2019: 2×10^7 qubits. In 2025: 10^6 qubits. Meanwhile, the largest quantum hardware has grown from ~50 qubits in 2017 to ~1000 qubits in 2023, and possibly modules of thousands by 2026. If we extrapolate this interplay for another few cycles, we converge on an intersection: by around the end of this decade, we might have machines with of order 10^5–10^6 physical qubits (thanks to modular scaling), and the algorithmic requirements might have shrunk to the same. IBM essentially confirmed this convergence by stating their 2029 machine (200 logical qubits) should be at the cusp of quantum advantage and presumably could be expanded to cryptanalysis tasks. My estimate of "Q-Day ~2030" assumes that no extraordinary roadblocks emerge in scaling quantum systems. It also assumes no further miraculous algorithmic leaps that would pull the date even closer (2030 is already quite soon given today's state, but I'm comfortable with it given the rate of progress).

How does this align with others' views? Surveys of experts have typically given a wide range: low probability in the 2020s, rising in the 2030s, and majority confidence by 2035. In other words, the consensus has been "sometime in the 2030s" with uncertainty on the exact year. My 2030 call is on the early edge of that consensus – arguably a bit more urgent. Why? Because the developments of the last two years (2023–2025), and especially last few weeks (no poll covered experts since), have all skewed towards sooner rather than later: breakthroughs in reducing qubit needs, improving error rates, and accelerating investment have tightened the timeline. If you asked me in 2020, I'd have said maybe 2035–2040. By 2022, seeing the pace, I moved to 2032. Now with the evidence at hand, I'm comfortable saying 2030 is a realistic target barring unforeseen slowdowns. And keep in mind, this isn't a guarantee – it's about risk. I'd characterize it like this: there is a non-trivial (say 30-50%) chance of a CRQC by 2030, rising to near certainty by 2035. That's enough to act on, especially given the stakes.

It's worth mentioning that Q-Day might not announce itself with fanfare. The first time RSA-2048 is factored by a quantum computer could very well happen in a classified lab or a clandestine project, with results kept secret. Alternatively, it might be a public demonstration by a company or research team to prove a point (much like the 1990s demonstrations of breaking 56-bit DES encryption – done to convince the world it was breakable). If it's the latter, we might get a heads-up like "*Today, researchers have factored RSA-2048 using a quantum computer, in a calculation that took X days on Y qubits*." If it's the former (e.g., a nation-state doing it quietly), we may not know Q-Day has arrived until much later (when perhaps leaked or when encrypted data starts getting mysteriously decrypted). The prudent course, of course, is to assume Q-Day could effectively come as soon as the technology is capable of it, whether or not it's widely announced.

To be clear, when I say "*RSA-2048 will be broken by 2030*," I am referring to a *demonstration of factoring a 2048-bit number with a quantum computer*. This is the canonical definition of Q-Day because RSA-2048 is a standard benchmark for public-key cryptography strength. But a CRQC would equally threaten other cryptosystems of similar or lesser strength: for instance, 256-bit elliptic curve (like the curves securing Bitcoin and many HTTPS connections) would also fall to Shor's algorithm with roughly the same order of effort. In fact, breaking a 256-bit EC key is a bit easier than 2048-bit RSA in theory (fewer qubits needed), so an RSA-breaking quantum computer certainly breaks ECC too. Diffie-Hellman key exchange, DSA, and any finite-field or elliptic curve system – all would be vulnerable. So Q-Day is not just about RSA; it's about the collapse of essentially all traditional public-key crypto. Symmetric crypto (AES, etc.) is less affected – Grover's quantum algorithm can speed up brute force attacks, but doubling key sizes mitigates that. The real catastrophe is in our asymmetric crypto infrastructure. Thus, when I say RSA-2048 will be broken, it's shorthand for "*our current public-key algorithms (RSA/ECC/DH) will no longer be safe*."

Now, some might argue: even if a million-qubit machine exists by 2030, running it to factor a large number might still be an arduous task – maybe it'll take weeks or months of runtime, maybe only nation-states will have the capability, etc. All true. But from a defensive standpoint, that's irrelevant. If a quantum computer can break your encryption given enough time, the encryption is effectively broken. Also, the technology curves only improve from there – what takes a nation-state weeks in 2030 could take a university days in 2035 and a script kiddie minutes by 2040, to exaggerate only slightly. The key point for decision-makers is that the risk becomes real the moment someone, somewhere, can do it at all. And that moment is approaching rapidly.

Here it's useful to invoke Mosca's rule, coined by Dr. Michele Mosca: if X = the years you need your data secure, Y = the years to deploy new crypto, and Z = the years before quantum breaks your crypto, then if X + Y > Z, you're in trouble. For many organizations, X (data confidentiality requirement) might be 5–10 years or more, and Y (upgrade time) is also several years. So if there's even a decent chance Z (Q-Day) is less than ~10-15 years out, you have a serious risk to address now. With 2030 as a credible target (just ~5 years from now for first capability, ~10 years for broader availability), X+Y for most should be greater than Z – meaning we're already in the danger zone. Indeed, NSA and NIST effectively acknowledged this: NIST's guidance is to begin migrating immediately and have quantum-vulnerable crypto deprecated by 2030. The U.S. government's national security systems are mandated to switch to post-quantum algorithms in the next few years (with NSA setting deadlines in the mid-2020s for starting the transition). These timelines weren't picked arbitrarily; they were based on risk assessments that essentially assume a CRQC might exist by the early-to-mid 2030s. With recent advances, those assumptions look even more valid, if not conservative.

Let's also address the outliers: the doomsayers and the nay-sayers. On one end, you have sensational claims that Q-Day is "next year" or "already here in secret." As of now, there's no credible evidence that anyone has a quantum computer powerful enough to threaten RSA-2048 in 2025 or 2026. We still struggle to keep just a few logical qubits alive. So, no, the sky isn't falling in 2025 or 2026 – don't let vendor marketing or hyperbolic media convince you otherwise. On the other end, you have respected cryptographers or physicists who remain deeply skeptical, saying things like "*quantum computers will never be scalable*" or "*we won't see this for many decades, if ever.*" I think the progress detailed in this article is a strong rebuttal to the extreme skeptics. We've seen too many "impossible" milestones reached in the last few years to claim it'll never happen. The conversation has shifted from "if" to "when" – even the cautious experts concede it's a matter of time (with second half of 2030s as an outside guess). In my view, clinging to "never" is wishful thinking that could leave you badly exposed if wrong. History of technology is full of examples where breakthroughs came sooner than anticipated once a field hit an exponential growth phase – and quantum computing appears to be at the cusp of such a phase right now.

So 2030 it is. Perhaps I'll be off by a couple of years – nobody can pinpoint the exact year with certainty. But as someone responsible for protecting data, you have to plan for the worst plausible case consistent with evidence. And the evidence now says the worst plausible case is only a handful of years away, not decades.

Conclusion

If there's one message to take away, it's this: the quantum threat to cryptography is no longer a distant abstraction; it's a tangible and approaching reality. Whether Q-Day arrives in 2028, 2030, or 2033, the difference is marginal – all are soon enough that we must prepare today. From the discussion above, a few key points stand out for security professionals and policymakers:

- **The Quantum Attack Trajectory is Shortening:** In 2012, breaking RSA-2048 needed a billion qubits – effectively impossible. By 2019, 20 million qubits. Now it's around one million qubits and a few days of runtime. This trend of improved algorithms and error correction is likely to continue. We can't bank on RSA's safety by saying "quantum computers need too many qubits" – that number keeps dropping. Assume that what looks infeasible now will become feasible sooner than expected; recent breakthroughs are proof of that dynamic.

- **Advances in Hardware are Accelerating:** Real experiments have demonstrated core requirements of a CRQC: logical qubits with error correction, 99.99999% fidelity gates, and multi-chip quantum processors in the works. Industry leaders and government programs are pouring resources into scaling up. Multiple credible roadmaps target the early 2030s for large-scale quantum machines capable of cryptanalysis. This is not science fiction – it's the explicit goal of IBM, Google, and others, with progress milestones being hit each year.

- **PQC Transition is Urgent and Unavoidable:** If anyone still doubted whether to invest in post-quantum cryptography (PQC) migration, these developments should erase that doubt. We now have NIST-standardized PQC algorithms (like CRYSTALS-Kyber, Dilithium, etc.), and major tech firms have begun implementing them (Google, Cloudflare, AWS, etc., are testing PQC in protocols and services). NIST's recommended timeline is to start phasing out vulnerable crypto by 2030, and completely eliminate it by 2035. That timeline wasn't picked casually – it aligns with when a quantum threat becomes not just possible but probable. Given the lead time required to transition systems (which can be 5-10 years for large enterprises or government agencies), starting now is the only viable strategy. Every year of delay increases the risk of being caught by Q-Day before you've finished upgrading. Remember, cryptographic agility (the ability to swap out algorithms) is part of resilience. If you haven't inventoried where you use RSA/ECC and developed a migration plan, you're already behind.

- "**Store Now, Decrypt Later**" **is a Real Threat:** Data that is encrypted today can be recorded by adversaries and kept until they have a quantum computer to decrypt it. This especially affects sensitive data with long confidentiality needs – think national security intelligence, healthcare records, confidential business plans, personal data protected by privacy laws, etc. If such data has a shelf life of more than ~5-10 years, assume that anything encrypted with RSA/ECC today might be readable by the 2030s. The only defense is to either stop using vulnerable encryption now for long-term data, or if that's not possible, shorten the lifetime of your secrets (e.g., enforce secure deletion or rotation so the data doesn't exist by the time a quantum attack could happen).

- **Don't Panic, but Do Prepare (Starting Yesterday):** The goal of highlighting Q-Day is not to incite fear but to promote action. We have solutions (PQC algorithms), and we have time if we use it wisely. The transition will be complex – some PQC algorithms have larger keys or signatures, meaning performance and compatibility issues need to be worked through. There will be new implementation bugs to watch for, and possibly further rounds of standardization (especially for digital signatures, where current PQC options are less mature). But these are solvable engineering challenges, and they are far preferable to the nightmare of waking up one day to find adversaries can trivially break all your encrypted traffic and stored communications. The recent breakthroughs serve as an exclamation point on earlier warnings: the clock is ticking.

To sum up, my updated Q-Day prediction of 2030 is not a prophecy set in stone, but a rational analysis of where current trends are heading. Whether I'm off by a couple years either way doesn't change the core advice. We are roughly five years out from the first potential quantum disruptions to cryptography, and about ten years out from them becoming widespread. This is within the horizon of strategic IT planning. It means every organization's 5-year roadmap should include quantum readiness. We're essentially in the final countdown to Y2Q – akin to the final stretch before Y2K, except this "millennium bug" for encryption doesn't have a fixed date and won't announce itself in advance. The prudent course is to act as if Q-Day will hit in the early 2030s, because the cost of being prepared a little early is far lower than the cost of being even one day late.

20. Futurex's PQC-HSM is PCI SSC validated for quantum security

by Ritesh Kumar
https://www.bisinfotech.com/futurexs-pqc-hsm-is-pci-ssc-validated-for-quantum-security/

As the only hardware security modules (HSMs) supporting PQC that have received PCI HSM validation, Futurex, a leader in enterprise data security worldwide, announced its accomplishment. Futurex's dedication to developing secure payment systems and guaranteeing preparedness for the changing dangers posed by quantum computing is demonstrated by this historic accreditation.

Advanced post-quantum cryptographic algorithms, such as ML-DSA (Message Length Digital Signature Algorithm) and ML-KEM (Message Length Key Encapsulation Mechanism), have been implemented by Futurex's HSMs, while SLH-DSA (Short Lattice Hash Digital Signature Algorithm) is about to be released. Once approved by NIST, Futurex's swift implementation of these methods will further solidify its position as a pioneer in cryptography innovation and payment ecosystem compliance.

"As the payments industry faces unprecedented challenges from quantum computing advancements, Futurex is at the forefront of securing sensitive data with cryptographic solutions that meet and exceed the latest PCI standards," said Abby Smith, CEO of Futurex. "Being the only HSM supporting PQC that has been PCI HSM validated demonstrates our dedication to providing our customers with the tools they need to future-proof their payment infrastructures."

Futurex offers unparalleled security and scalability with its HSMs, which are part of its PQC package and comply with FIPS 203 and 204 standards. This further demonstrates Futurex's capacity to safeguard payment systems, protect data while it's in transit and at rest, and guarantee adherence to international security standards.

Addressing Quantum Computing Challenges in Payments

A revolutionary technical advancement, quantum computing has the ability to crack conventional encryption techniques. By using cryptographic algorithms that are resistant to quantum assaults, Futurex's PQC-ready solutions proactively mitigate these risks and guarantee safe transactions in a variety of payment contexts.

Upgrades to both on-premises and cloud-based Futurex solutions can enable PQC capabilities, guaranteeing that all payment workloads remain secure both now and in the future.

A strategy called Harvest Now, Decrypt Later (HNDL) is being used by cybercriminals. They anticipate that future developments in quantum computing would undermine existing safeguards, therefore they target and store vast amounts of data that are encrypted using current standards.

Cryptographic solutions are thoroughly assessed as part of the PCI SSC certification process to guarantee their robustness in payment applications. Futurex's accomplishment demonstrates its position as a reliable partner for businesses looking to improve payment security while satisfying changing legal requirements.

Commitment to Innovation and Industry Standards

As a leader in cryptography technology, Futurex has established a reputation for regularly hitting first-to-market benchmarks that raise the bar for the sector. Futurex has tackled enterprise issues in tokenisation, key management, and data encryption globally, from launching cloud and virtualised HSMs to integrating payment and general-purpose HSMs. Futurex's continuous cooperation with industry standards organisations, such as the PCI SSC, to create and implement safe, scalable solutions for the payments industry is reflected in this most recent accreditation.

21. Getting Ready for a Secure AI and Post-Quantum World

by Takanori Nishiyama
https://technode.global/2025/06/20/getting-ready-for-a-secure-ai-and-post-quantum-world/

Artificial Intelligence (AI) has become deeply embedded in our daily lives – from smartphone photo enhancements to automated meeting summaries and hyper-realistic video content. In the workplace, AI is fueling productivity, creativity, and communication. But while businesses embrace its potential, threat actors are doing the same.

The AI-enhanced threat landscape

As AI becomes more accessible, cybercriminals are using it to launch faster, more convincing attacks. Deepfake videos, AI-generated phishing emails, and social engineering campaigns are now more personalized and harder to detect. Attackers can quickly scan public data, mimic real people, and create realistic videos, voices, and messages that trick users into sharing sensitive information or credentials.

To stay ahead, organizations need a layered security approach – one that doesn't rely on a single tool or solution, but instead uses multiple defenses working together. This strategy helps block threats at different points, limits damage if an attack does happen, and improves overall resilience.

A few key layers stand out:

- AI-powered threat detection helps organizations spot unusual activity in real time, such as suspicious logins or phishing attempts. These tools can catch what traditional systems might miss and respond faster than a human team alone.

- Zero-trust security means never automatically trusting users or devices, even if they're inside the network. Every access request is verified, and access is limited to only what's necessary, reducing the chance of attackers moving freely once inside.

- Privileged Access Management (PAM) protects high-level accounts that could do the most damage if compromised. By limiting who can access sensitive systems and when, PAM helps prevent attackers from escalating their privileges or reaching critical IT infrastructure.

No one solution is enough on its own, but together, these tools and strategies form a strong foundation. As attackers grow more advanced with AI, defenders must do the same, with smart tools, smart strategies, and a focus on reducing risk from all angles.

Quantum computing and the next wave of threats

Quantum computing is no longer a far-off concept – it's becoming a reality with real-world implications for cybersecurity. Its development poses a serious threat to traditional encryption methods like RSA and elliptic curve cryptography. Governments and institutions worldwide, including in Japan, are already responding.

The Japanese Financial Services Agency has encouraged banks to explore Quantum-Resistant Cryptography (QRC), and National Institute of Standards and Technology (NIST) in the U.S. has released new post-quantum cryptographic standards.

The "store now, decrypt later" threat is real – where attackers harvest encrypted data today in hopes of decrypting it with quantum computers tomorrow. Transitioning to quantum-resistant encryption takes time, and organizations – particularly those in finance, healthcare, and government – should begin evaluating QRC solutions now as part of their long-term cybersecurity strategy.

The role of standards

In today's hyper-connected digital landscape, cybersecurity isn't just about protecting your own organization – it's also about ensuring the security of everyone you do business with. That's why internationally recognized standards, like ISO 27001, are critical not only for internal operations but also when selecting technology vendors and business partners.

ISO 27001 provides a globally accepted framework for establishing and maintaining an Information Security Management System (ISMS). It ensures organizations have the policies, processes, and controls in place to manage risks and protect sensitive data. Achieving ISO 27001 certification demonstrates a serious, ongoing commitment to cybersecurity and data protection.

For enterprises, implementing ISO 27001 internally helps strengthen governance, align with regulatory requirements, and build resilience against evolving threats. But it shouldn't stop there. Organizations should also expect the same standard of security from the vendors, suppliers, and partners they work with – especially those that handle sensitive systems, data, or infrastructure.

Working with ISO 27001-certified vendors provides greater transparency and assurance that best practices are being followed throughout your extended ecosystem. Without these assurances, even a well-protected organization can be put at risk by a less secure third party.

In short, standards matter – and they should apply across the entire supply chain. A proactive approach to security means not just protecting your own house, but also making sure everyone you depend on is doing the same.

A secure future with AI

AI can be a force for good – when paired with strong cybersecurity practices. As organizations adopt generative AI tools and agents, they must also adopt modern defenses: PAM, zero-trust principles, quantum-resistant cryptography, employee education, and globally recognized standards. Cybersecurity is not a checkbox; it's a continuous journey. And with the pace of innovation, the time to act is now.

22.Quantum Computing: choppy waters ahead

by R V Raghu
https://timestech.in/quantum-computing-choppy-waters-ahead/

Along with AI, quantum computing is a key technology poised to upend the world as we know it. The transformational capacity of quantum computing is enormous, with a wide range of applications including faster data analysis, accelerating AI and unlocking new business opportunities. But despite these and other benefits, enterprises are very poorly prepared for the paradigm shift quantum computing is expected to bring.

ISACA's 2025 Quantum Computing Pulse Poll revealed a whopping 92% of organizations in India lack a quantum computing strategy, while 38% of organizations have not even begun to take steps to prepare for quantum computing. This is deeply concerning with 53% of India-based technology and cybersecurity experts believing quantum computing could soon compromise today's encryption standards before browsers and websites fully implement new post quantum cryptography algorithms, leaving a gap hole in the security postures. Quantum computing can also break today's cryptographic algorithms, which underpin nearly all online transactions, digital signatures, web sites, utilities, medical records and other critical systems. The threat of "harvest now, decrypt later"– where cybercriminals stockpile encrypted data for future decryption using quantum power – also weighs heavily, flagged by 51% of those surveyed in India.

Despite these and other risks, many organizations are underprepared for a world of quantum computing and need to closely relook at their strategies for a post quantum world with specific emphasis on whether they have the expertise to implement necessary solutions for a post quantum world.

40% of organizations in India believe the transformative potential of quantum computing will be realized within the next five years, underscoring the urgency of action. However, 19% of respondents in India admitted they have no awareness of their company's planned or current use of quantum computing and a striking 33% confirmed their companies have not discussed quantum computing at all.

The strategy gap is also yawning. Only 9% of organizations in India consider quantum computing a high-priority area for near-term planning, and only 25% have placed it on their long-term roadmap. Additionally, 33% report that the topic hasn't been discussed at all within their organizations.

Though this is all concerning, there are actions that enterprises can start taking now – and the sooner the better:

- Educating stakeholders about quantum computing's risks and the urgent need for quantum-resistant encryption.
- Developing a quantum computing encryption strategy for new and existing data.
- Assessing and identifying where encrypted data are stored; determine vulnerabilities.
- Begin transitioning critical data and systems to quantum-resistant encryption.
- Upgrading digital infrastructure, ensure all Internet-connected systems are secure.

- Assessing regulatory and compliance implications.
- Collaborating with quantum hardware and software providers or consortia.
- Investing in research, development, and proof-of-concept projects relating to quantum computing.
- Finally, conducting regular audits and readiness assessments.

Enterprises and practitioners would well build a sense of urgency around quantum computing initiatives. It is not a matter of *if* but *when* quantum computing will go mainstream, and no one wants to be caught unprepared because the cost will be too high.

23. DRDO & IIT Delhi Demonstrate Quantum Entanglement-Based Free-Space Quantum Secure Communication over more than 1 km Distance

by PIB
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2136702

India has entered into a new quantum era by successfully demonstrating an experimental advancement through DRDO-Industry-Academia Centre of Excellence (DIA-CoE), IIT Delhi. The free-space quantum secure communication using quantum entanglement over a distance of more than one km was achieved via a free-space optical link established on the IIT Delhi campus.

The experiment attained a secure key rate of nearly 240 bits per second with a quantum bit error rate of less than 7%. This entanglement-assisted quantum secure communication paves the way for real-time applications in quantum cyber security, including long-distance Quantum Key Distribution (QKD), the development of quantum networks, and the future quantum internet. These efforts align with India's broader objectives to advance quantum technologies for national development.Under the project 'Design and development of photonic technologies for free space QKD', sanctioned by Directorate of Futuristic Technology Management (DFTM), DRDO, the demonstration was given by Prof Bhaskar Kanseri's research group in the presence of several dignitaries, including the DRDO DG (MED, COS & CS), Director SAG, Director DFTM, Dean (R&D) IIT Delhi, Director (DIA-CoE) and DRDO laboratory scientists.

Quantum entanglement-based QKD offers several significant advantages over the traditional prepare-and-measure method by enhancing both security and functionality. Even if devices are compromised or imperfect, the use of quantum entanglement ensures the security of key distribution. Any attempt to measure or intercept the entangled photons disturbs the quantum state, allowing authorised users to detect the presence of an eavesdropper.

Quantum communication provides fundamentally unbreakable encryption, making it a dual-use technology with applications in securing data in strategic sectors such as defence, finance, and telecommunications, as well as in protecting national security-related communications. Free-space QKD eliminates the need to lay optical fibers, which can be both disruptive and expensive, especially in challenging terrains and dense urban environments.

Earlier, India’s first intercity quantum communication link between Vindhyachal and Prayagraj in 2022, using commercial-grade underground dark optical fiber was demonstrated by DRDO scientists along with Prof Bhaskar’s team. More recently, in 2024, the team successfully distributed quantum keys using entanglement over a 100 km spool of telecom-grade optical fiber in another DRDO-supported project.

These technologies are being developed through DRDO-Industry-Academia – Centres of Excellence (DIA-CoEs) – an initiative of DRDO, where 15 Centres of Excellence have been established at premier academic institutes like IITs, IISc & Universities for development of cutting edge defence technologies.

Raksha Mantri Shri Rajnath Singh has congratulated DRDO & IIT Delhi for this landmark achievement, stating that India entered into a new quantum era of secure communication which will be a game changer in future warfare.

Secretary Department of Defence R&D and Chairman DRDO Dr Samir V Kamat and Director, IIT Delhi Prof Rangan Banerjee congratulated the team for these key achievements.

24. Quantum Computing Spurs Urgency on Cryptography Upgrades

by Michael Novinson
https://www.govinfosecurity.com/quantum-computing-spurs-urgency-on-cryptography-upgrades-a-28656

The real and present quantum computing danger comes from adversaries harvesting data now and decrypting it once computers are capable of breaking RSA encryption, experts said.

Both Amazon Web Services and Accenture are actively helping organizations transition to post-quantum computing by 2030 to 2035 in accordance with NIST recommendations. AWS has doubled down on advanced infrastructure, services and open-source cryptography modules, while Accenture has focused on consultative and experimental approaches including quantum security in space, executives said.

"The near-term concern for most organizations is, 'When is a quantum computer going to be a realistic threat to my data security?'" said Scott Francis, emerging technology security lead at Accenture. "And the answer to that is dependent on how long it's going to take before a quantum computer can factor RSA, which is the underpinning of most of what we use for public key cryptography on the internet."

In this video interview with Information Security Media Group, Francis and AWS Solution Architect Rajdeep Banerjee also discussed:

- The risk landscape, "harvest now, decrypt later" threats and regulatory drivers;
- Business and technological implications of quantum computing;
- Advice for firms beginning post-quantum computing transition;

Banerjee has more than 19 years of software industry experience spanning software development, technology consulting and cloud architecture. He supports partners and customers in their cloud migration journey and technology stack modernization. He helps customers establish secure cloud environments through foundational landing zones, security and compliance controls, and continuous monitoring solutions.

Francis leads Accenture's emerging tech security practice in the Americas. He has been designing, building, operating and securing Internet-facing services for organizations of all sizes, in industries around the world, since the '90s. He is pathologically curious, and his focus for many years has included emerging technology and the fascinating (and unexpected) things that happen where domains overlap.

25. NIST and Partners Use Quantum Mechanics to Make a Factory for Random Numbers

by Rebecca Jacobson
https://www.nist.gov/news-events/news/2025/06/nist-and-partners-use-quantum-mechanics-make-factory-random-numbers

Randomness is incredibly useful. People often draw straws, throw dice or flip coins to make fair choices. Random numbers can enable auditors to make completely unbiased selections. Randomness is also key in security; if a password or code is an unguessable string of numbers, it’s harder to crack. Many of our cryptographic systems today use random number generators to produce secure keys.

But how do you know that a random number is truly random? Classical computer algorithms can only create pseudo-random numbers, and someone with enough knowledge of the algorithm or the system could manipulate it or predict the next number. An expert in sleight of hand could rig a coin flip to guarantee a heads or tails result. Even the most careful coin flips can have bias; with enough study, their outcomes could be predicted.

“True randomness is something that nothing in the universe can predict in advance,” said Krister Shalm, a physicist at the NIST. Even if a random number generator used seemingly random processes in nature, it would be hard to verify that those numbers are truly random, Shalm added.

Einstein believed that nature isn’t random, famously saying, “God does not play dice with the universe.” Scientists have since proved that Einstein was wrong. Unlike dice or computer algorithms, quantum mechanics is inherently random. Carrying out a quantum experiment called a Bell test, Shalm and his team have transformed this source of true quantum randomness into a traceable and certifiable random-number service. Their results were just published in *Nature*.

“If God does play dice with the universe, then you can turn that into the best random number generator that the universe allows,” Shalm said. “We really wanted to take that experiment out of the lab and turn it into a useful public service.”

To make that happen, NIST researchers and their colleagues at the University of Colorado Boulder created the Colorado University Randomness Beacon (CURBy). CURBy produces random numbers automatically and broadcasts them daily through a website for anyone to use.

At the heart of this service is the NIST-run Bell test, which provides truly random results. This randomness acts as a kind of raw material that the rest of the researchers' setup "refines" into random numbers published by the beacon.

The Bell test measures pairs of "entangled" photons whose properties are correlated even when separated by vast distances. When researchers measure an individual particle, the outcome is random, but the properties of the pair are more correlated than classical physics allows, enabling researchers to verify the randomness. Einstein called this quantum nonlocality "spooky action at a distance."

This is the first random number generator service to use quantum nonlocality as a source of its numbers, and the most transparent source of random numbers to date. That's because the results are certifiable and traceable to a greater extent than ever before.

"CURBy is one of the first publicly available services that operates with a provable quantum advantage. That's a big milestone for us," Shalm explained. "The quality and origin of these random bits can be directly certified in a way that conventional random number generators are unable to."

NIST performed one of the first complete experimental Bell tests in 2015, which firmly established that quantum mechanics is truly random. In 2018, NIST pioneered methods to use these Bell tests to build the world's first sources of true randomness.

However, turning these quantum correlations into random numbers is hard work. NIST's first breakthrough demonstrations of the Bell test required months of setup to run for a few hours, and it took a great deal of time to collect enough data to generate 512 bits of true randomness. Shalm and the team spent the past few years building the experiment to be robust and to run automatically so it can provide random numbers on demand. In its first 40 days of operation, the protocol produced random numbers 7,434 times out of 7,454 attempts, a 99.7% success rate.

The process starts by generating a pair of entangled photons inside a special nonlinear crystal. The photons travel via optical fiber to separate labs at opposite ends of the hall. Once the photons reach the labs, their polarizations are measured. The outcomes of these measurements are truly random. This process is repeated 250,000 times per second.

NIST passes millions of these quantum coin flips to a computer program at the University of Colorado Boulder. Special processing steps and strict protocols are used to turn the outcomes of the quantum measurements on entangled photons into 512 random bits of binary code (0s and 1s). The result is a set of random bits that no one, not even Einstein, could have predicted. In some sense, this system acts as the universe's best coin flip.

NIST and its collaborators added the ability to trace and verify every step in the randomness generation process. They developed the Twine protocol, a novel set of quantum-compatible blockchain technologies that enable multiple different entities to work together to generate and certify the randomness from the Bell test. The Twine protocol marks each set of data for the beacon with a hash. Hashes are used in blockchain technology to mark sets of data with a digital fingerprint, allowing each block of data to be identified and scrutinized.

The Twine protocol allows any user to verify the data behind each random number, explained Jasper Palfree, a research assistant on the project at the University of Colorado Boulder. The protocol can expand to let other random number beacons join the hash graph, creating a network of randomness that everyone contributes to but no individual controls.

Intertwining these hash chains acts as a timestamp, linking the data for the beacon together into a traceable data structure. It also provides security, allowing Twine protocol participants to immediately spot manipulation of the data.

“The Twine protocol lets us weave together all these other beacons into a tapestry of trust,” Palfree added. Turning a complex quantum physics problem into a public service is exactly why this work appealed to Gautam Kavuri, a graduate student on the project. The whole process is open source and available to the public, allowing anyone to not only check their work, but even build on the beacon to create their own random number generator.

CURBy can be used anywhere an independent, public source of random numbers would be useful, such as selecting jury candidates, making a random selection for an audit, or assigning resources through a public lottery.

“I wanted to build something that is useful. It’s this cool thing that is the cutting edge of fundamental science,” Kavuri added. “NIST is a place where you have that freedom to pursue projects that are ambitious but also will give you something useful.”

26. Security without sacrifice: Threshold cryptography and the future of wallet UX

by Erick Watson
https://www.bobsguide.com/threshold-cryptography-and-the-future-of-wallet-ux/

Today’s digital landscape presents a paradox as users demand seamless, frictionless experiences while simultaneously expecting airtight security for their digital assets and sensitive information. Unfortunately, conventional methods often force users into an uncomfortable tradeoff: simplicity at the cost of security, or vice versa. Emerging solutions, however, leveraging threshold cryptography, present a compelling vision where security no longer has to compromise usability. This technology could redefine wallet experiences, enabling a near-future where losing your phone doesn’t mean losing your funds, and where hacks like bridge thefts become far less commonplace.

The security-usability tradeoff in wallets today

Historically, security measures for digital wallets and asset storage have been cumbersome, complex, and daunting for everyday users. Strong security typically requires managing private keys or memorizing complicated seed phrases, practices that discourage mainstream adoption and leave users vulnerable to human error. On the other hand, easy-to-use platforms often come with reduced security, as they centralize assets on vulnerable custodial services or rely on weak authentication methods. Unfortunately, many current wallet approaches tilt to one side of the balance:

- Custodial wallets manage private keys for users, making crypto as easy to use as traditional banking apps, but users must trust the provider. When that trust is breached, the results are catastrophic. High-profile breaches have shown that a single compromised key or password can drain thousands of user accounts in one stroke.

- Non-custodial wallets enable users to hold their own keys, thereby avoiding centralized risks, but place the full burden on individuals to manage them. Human error looms large, with lost access seed phrases, phishing scams, and insecure backups resulting in billions of dollars in losses. Complex multi-signature setups and hardware devices exist to mitigate these risks, but they can be awkward and intimidating for everyday users.

Threshold cryptography emerges as a transformative approach that can bridge this gap. By dividing cryptographic keys into secure fragments and distributing them among multiple parties, this technology dramatically enhances security without burdening the user with complex key management.

Threshold cryptography demystified

At its core, threshold cryptography splits sensitive keys into multiple fragments, requiring only a subset (or threshold) of those fragments to authorize transactions or perform recovery actions. For instance, a wallet's key might be fragmented into five parts, stored with separate trusted entities or devices. Transactions or recovery procedures might require any three of these fragments. Crucially, these cryptographic protocols never reconstruct the full private key in a single location. This method ensures resilience, eliminating single points of failure and substantially reducing the risk of key loss or theft.

Unlike traditional multi-signature methods, threshold cryptography doesn't require numerous signatures from different parties. Instead, it recombines fragments mathematically into one single valid signature. This simplifies interactions, minimizes on-chain costs, and ensures speed and user convenience while maintaining high security.

Enterprise and institutional custodians have already embraced threshold cryptography to secure large holdings. Many banks and fintech firms exploring crypto custody are opting for Multi Party Compute (MPC) based wallets. These solutions enable multiple approvers and flexible policies (e.g., requiring three of five senior officers to co-sign a transfer) without relying on costly, slow, blockchain-specific multi-signature scripts. The result is bank-grade security that's invisible to the end-user. As this technology matures and trickles down, retail users stand to benefit from the same security without sacrificing convenience in their everyday wallets.

Reimagining wallet UX: convenience and security in harmony

Imagine a near-future wallet experience that provides the same intuitive ease as tapping a contactless payment card, yet offers enterprise-grade security. Here's how threshold cryptography could make this reality achievable.

Trusted Contacts as Custodians

In a threshold wallet system, fragments of your cryptographic keys could reside securely with trusted contacts, family members, institutions, or separate devices you control. Unlike centralized custody, this distributed custody model significantly mitigates the risks of hacks or single-point-of-failure events.

Automated Recovery Policies

Losing a device or forgetting a password no longer spells disaster. Threshold cryptography can automate recovery policies, allowing users to regain access with minimal friction. For example, recovering access could involve a simple confirmation tap on a device belonging to a trusted contact or institution holding a key fragment that requires a 48-hour waiting period for a reset. This reduces anxiety around key management and enhances the practicality of secure wallets.

One-Tap Convenience

Leveraging threshold cryptography, wallet transactions can maintain simplicity with the familiar one-tap confirmation paradigm. Users authorize payments or access assets instantly, with underlying cryptographic security invisible yet robustly active in the background. This seamless experience makes advanced security intuitive and user-friendly.

Real-world application scenarios

Threshold wallets have numerous uses across financial services, extending beyond cryptocurrency into mainstream banking, asset management, and identity verification:

Retail Banking: Banks can offer their customers highly secure, user-friendly wallets to safely store digital currencies, equities, or bonds, thereby significantly reducing fraud and enhancing customer trust.

Insurance and Wealth Management: Advisors and clients can jointly manage assets through distributed key fragments, streamlining approvals while securing sensitive portfolios from unauthorized access.

Payments and Remittances: Threshold-based wallets simplify international payments, eliminating complex authentication processes while maintaining stringent security standards and baked-in compliance logic.

Overcoming adoption barriers

Despite its advantages, widespread adoption of threshold cryptography-based wallets requires addressing several challenges:

Education and Awareness: The finance and technology sectors must prioritize user education to build trust and familiarity with new cryptographic methods.

Interoperability and Standards: Developing industry-wide standards will be essential to ensure interoperability across platforms, institutions, and devices.

Regulatory Alignment: Clear regulatory guidance will foster adoption, assuring compliance and providing confidence for mainstream financial institutions and users alike.

The road ahead: no longer choosing between security and simplicity

The future of wallet user experience lies in abstracting away the cumbersome aspects of security while actually enhancing the security under the hood. Threshold cryptography provides a powerful toolkit to achieve this. It allows us to resolve the age-old tradeoff between security and convenience by fundamentally changing how keys are managed. Instead of relying on a single key to guard or lose, we have collaborative security: multiple fragments, multiple participants, and automated policies that together protect users in a way no single key could ever do.

By adopting threshold cryptographic techniques, financial institutions and technology providers can fundamentally redefine customer experiences, enabling users to transact effortlessly with confidence in robust, invisible security measures. This isn't just about enhancing wallets, it's about reshaping trust in the digital age, making security an integral yet unobtrusive part of our daily lives.

Ultimately, threshold cryptography will help the fintech industry achieve what has long seemed impossible: enabling everyday users to enjoy both uncompromising security and unprecedented convenience.

27. President Trump Modifies Executive Order 14144 for Government PQC Migration

by GQI
https://quantumcomputingreport.com/president-trump-modifies-executive-order-14144-for-government-pqc-migration/

On January 17, 2025, President Biden issued Executive Order 14144 which covered among other things requirements for agencies to implement Post Quantum Cryptography (PQC) algorithms as soon as practicable. On June 6, 2025, President Trump signed an Executive Order modifying the original one to redirect efforts from proactive development to identifying and managing vulnerabilities, moving away from initiatives perceived as regulatory overreach.

Perhaps the best way to show the specific changes is to provide a marked-up version of the relevant subsection 4(f) in this order to show what has been added and deleted. You can view the original Executive Order 14144 published in January in the Federal Register here and the modifications that have just been made to it here. A Fact Sheet that provides an overview of the modifications made in the areas of cybersecurity related Executive Orders 14144 and 13694 can be accessed here.

Marked-Up Comparison

(f) ~~Alongside their benefits, quantum computers pose significant risk to the national security, including the economic security, of the United States. Most notably, a~~ A quantum computer of sufficient size and sophistication– – also known as a cryptanalytically relevant quantum computer (CRQC)–) – will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. In National Security Memorandum 10 of May 4, 2022 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems), I directed the Federal Government to prepare for a transition to cryptographic algorithms that would not be vulnerable to a CRQC.

(i) ~~Within 180 days of the date of this order~~ By December 1, 2025, the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and in consultation with the Director of the National Security Agency, shall release and thereafter regularly update a list of product categories in which products that support post-quantum cryptography (PQC) are widely available.

(ii) ~~Within 90 days of a product category being placed on the list described in subsection (f)(i) of this section, agencies shall take steps to include in any solicitations for products in that category a requirement that products support PQC~~.

(iii) ~~Agencies shall implement PQC key establishment or hybrid key establishment including a PQC algorithm as soon as practicable upon support being provided by network security products and services already deployed in their network architectures.~~

(iv) ~~Within 90 days of the date of this order, the Secretary of State and the Secretary of Commerce, acting through the Director of NIST and the Under Secretary for International Trade, shall identify and engage foreign governments and industry groups in key countries to encourage their transition to PQC algorithms standardized by NIST~~.

(v) ~~Within 180 days of the date of this order By December 1, 2025~~, to prepare for transition to PQC, the ~~Secretary of DefenseDirector of the National Security Agency~~ with respect to National Security Systems (NSS), and the Director of OMB with respect to non-NSS, shall each issue requirements for agencies to support, as soon as practicable, but not later than January 2, 2030, Transport Layer Security protocol version 1.3 or a successor version.

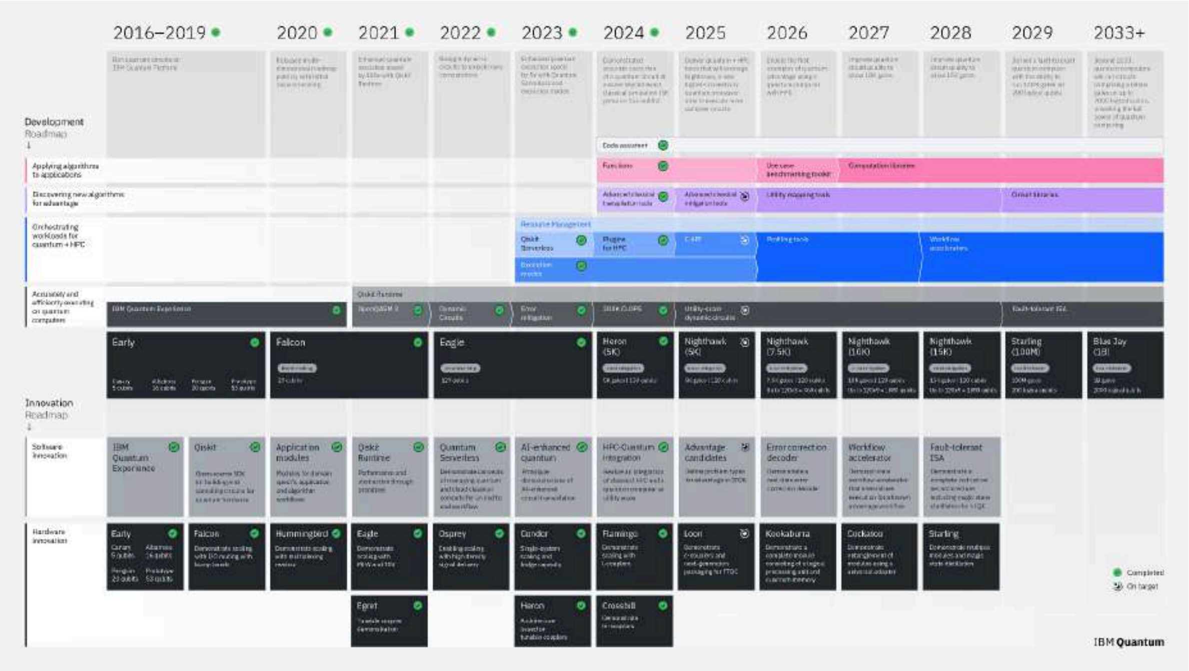
28. How IBM will build the world's first large-scale, fault-tolerant quantum computer

by Ryan Mandelbaum, Jay Gambetta, Jerry Chow, Tushar Mittal, Theodore J. Yoder, Andrew Cross, and Matthias Steffen
https://www.ibm.com/quantum/blog/large-scale-ftqc

With two new research papers and an updated quantum roadmap, IBM® lays out a clear, rigorous, comprehensive framework for realizing a large-scale, fault-tolerant quantum computer by 2029.

IBM has the most viable path to realize fault-tolerant quantum computing. By 2029, we will deliver IBM Quantum Starling — a large-scale, fault-tolerant quantum computer capable of running quantum circuits comprising 100 million quantum gates on 200 logical qubits. We are building this system at our historic facility in Poughkeepsie, New York.

In a new paper, now available on the arXiv, we detail a rigorous end-to-end framework for a fault-tolerant quantum computer that is modular and based on the bivariate bicycle codes we introduced with our landmark 2024 publication in *Nature*. Additionally, we're releasing a second paper that details the first-ever accurate, fast, compact, and flexible error correction decoder — one that is amenable to efficient implementation on FPGAs or ASICs for real-time decoding. We've updated our roadmap to match, with new processors and capabilities that will pave the way to quantum advantage, Starling, and fault tolerance.



Since 2020, IBM has worked transparently along its quantum roadmap, laying out the steps required to realize useful quantum computing. Recent revisions to that roadmap project a path to 2033 and beyond, and so far, we have successfully delivered on each of our milestones. Based on that past success, we feel confident in our continued progress.

In fact, from what we have seen, IBM is the only quantum computing organization in the world that will be capable of running quantum programs at the scale of hundreds of logical qubits and millions of quantum gates by the end of the decade.

What makes us so confident? Let us show you.

Building a fault-tolerant quantum computer

Today, IBM is a leader in quantum computing. Our quantum computers are the only ones capable of delivering accurate results for quantum circuits with 5,000+ two-qubit gates. Based on research with partners such as RIKEN, Boeing, Cleveland Clinic, and Oak Ridge National Laboratory, we feel confident that our users will deliver quantum advantage — solving problems cheaper, faster, or more efficiently than classical alone — by the end of 2026, with quantum serving as an accelerator for classical HPC.

However, current devices and error-mitigating techniques limit us to small circuits. Unlocking the full promise of quantum computing will require a device capable of running larger, deeper circuits with hundreds of millions of gates operating on hundreds of qubits, at least. More than that, it will require a device capable of correcting errors and preventing them from spreading throughout the system. In other words, it will require a fault-tolerant quantum computer.

In our new paper, we detail six essential criteria for realizing a scalable architecture for reliable, large-scale quantum computing, and we show how our "bicycle architecture" meets these criteria. They are as follows:

1. **Fault-tolerant.** Logical errors are suppressed enough for meaningful algorithms to succeed.
2. **Addressable.** Individual logical qubits can be prepared or measured throughout the computation.
3. **Universal.** A universal set of quantum instructions can be applied to the logical qubits.
4. **Adaptive.** Measurements are real-time decoded and can alter subsequent quantum instructions.
5. **Modular.** The hardware is distributed across a set of replaceable modules connected quantumly.
6. **Efficient.** Meaningful algorithms can be executed with reasonable physical resources.

Below, we'll lay out our architecture in more detail and explain how it meets these criteria. But before we do that, let's briefly review how we detect and correct errors that arise in quantum computers.

Correcting errors

Quantum error correction is the name for a family of techniques where we encode quantum information into physical qubits to protect them against errors. We do something similar in conventional computing. If we have three physical transistors and want to encode one binary digit's worth of information into them, then we could represent 0 as 000, and we could represent 1 as 111. We can define correction as majority voting – so even if one transistor errors, the encoded data isn't corrupted. Let's call 000 and 111 our three physical bits, and call the 0 and 1 they represent our logical bits.

Our goal is to do something similar in quantum computing – construct logical quantum bits, or qubits, from physical qubits. A physical qubit is a unit of well-isolated quantum computing hardware capable of being programmed and coupled to more than one other qubit in a controllable manner. A logical qubit is a qubit's worth of encoded information that can be made from one or more physical qubits, depending on the quantum error correction code.

We denote a quantum code's parameters by [[n, k, d]] where n is the number of physical data qubits required, k is the resulting number of logical qubits, and d is the distance of the code – how many errors it takes to silently corrupt the data encoded on the logical qubit (i.e., how many errors it takes to change an error-free encoded state to another encoded state that appears completely error-free). In a classical analog, you'd say the above code (0 = 000, 1 = 111) is a [3, 1, 3] code (note the single bracket for a classical code). An error correction code can correct up to (d-1)/2 errors and detect up to d-1 errors.

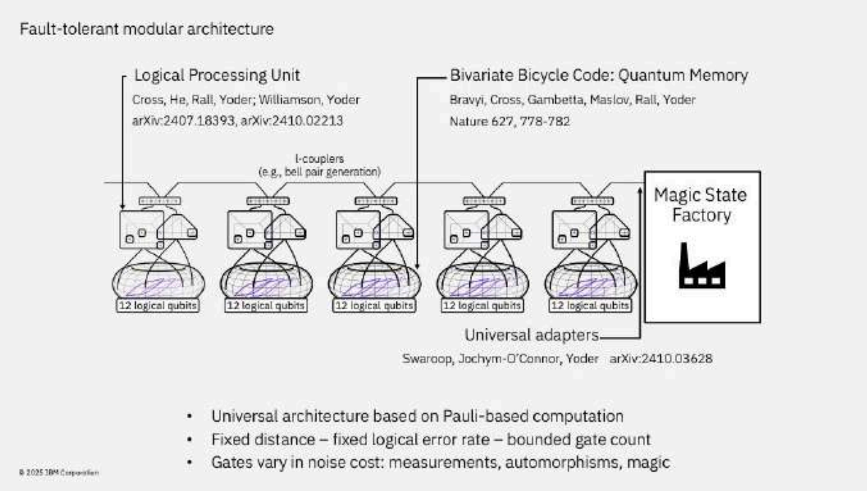
Just like classical computing, we can represent 0 and 1 as specific quantum states that incorporate multiple qubits. You might encode |00⟩ as |0000⟩+|1111⟩, |01⟩ as |1100⟩+|0011⟩, |10⟩ as |1010⟩+|0101⟩ and |11⟩ as |1001⟩+|0110⟩, for example. Then, we can monitor these qubits by regularly running error syndrome extraction circuits, which detect evidence of errors – for example, measuring an output with an odd number of 1s in the case described above would be an obvious error. Together, these make up what we call the quantum memory.

But you need more than a memory to compute. Quantum computing requires a universal gate set, or a set of logic gates to which every quantum computation can be reduced. Our universal gate set begins with a group of familiar gates called Clifford gates, which must run on the encoded information quickly and with limited overhead. It also requires at least one non-Clifford gate, such as the T gate, which is harder to realize. We apply T gates by creating special states called "magic states" on helper qubits, then we entangle these qubits into our circuits with Clifford gates.

We also need to be able to read out the logical qubits — for this, we use a tool called the decoder. This is classical hardware capable of reading the error syndromes, updating our beliefs about errors in real time, and outputting the corrected information. Finally, this whole system must be modular — it must scale to sizes large enough to run meaningful computations.

An architecture for realizing fault-tolerant quantum computing

Our new paper presents an architecture based on years of prior work, which meets these requirements for fault-tolerant quantum computing in a scalable system.



Fault-tolerant modular architecture

Logical Processing Unit
Cross, He, Rall, Yoder; Williamson, Yoder
arXiv:2407.18393, arXiv:2410.02213

Bivariate Bicycle Code: Quantum Memory
Bravyi, Cross, Gambetta, Maslov, Rall, Yoder
Nature 627, 778-782

Universal adapters
Swaroop, Jochym-O'Connor, Yoder arXiv:2410.03628

- Universal architecture based on Pauli-based computation
- Fixed distance – fixed logical error rate – bounded gate count
- Gates vary in noise cost: measurements, automorphisms, magic

© 2025 IBM Corporation

Let's walk through each step of that architecture. In 2024, we introduced a fault-tolerant quantum memory based on quantum low-density parity check (qLDPC) codes called bivariate bicycle (BB) codes. The [[144,12,12]] gross code encodes 12 logical qubits into 144 data qubits—a gross—along with another 144 syndrome check qubits, for a total of 288 physical qubits. This code corrects errors just as well as the surface code does, but requires 10x fewer qubits to do so.

Last year, our team and their collaborators discovered that we could build efficient, fault-tolerant logical processing units (LPUs) for qLDPC codes. These LPUs are based on a technique called generalized (lattice) surgery and have valuable properties: they perform logical measurements using low-weight checks, and do so with very few additional qubits. We can use LPUs together with the symmetries of the qLDPC code to perform logical stabilizer computations, such as Clifford gates, state preparations, and measurements. In our new paper[1], we design efficient LPUs for the gross code and a larger [[288,12,18]] BB code called the two-gross code that corrects more errors. The combined memory and LPU is one type of module in our architecture.

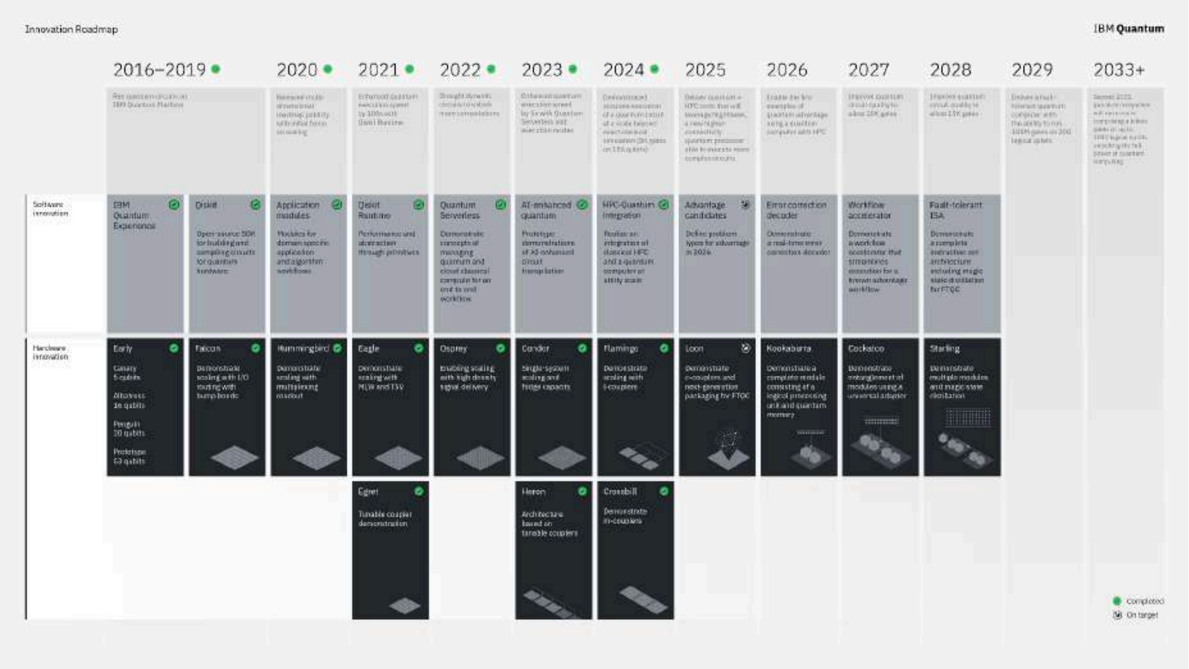
Our team and their collaborators also introduced concepts for universal adapters, which use bridges to interact and move logical quantum information between modules. Parts of the adapters can be implemented using the inter-module microwave l-couplers we first demonstrated last year with IBM Quantum Flamingo. Our new paper elaborates on the adapter construction and characterizes a baseline inter-module measurement instruction.

Universal computation can be done by augmenting logical stabilizer computations with magic state factories that create, distill, and consume magic states to apply universal gates. Sergey Bravyi and Alexei Kitaev invented the process of magic state distillation in 2004. Our team has made numerous contributions to the development of magic state preparation protocols since then, and in 2024, we published an experimental demonstration of such a protocol. Our new paper constructs explicit universal fault-tolerant instruction sets using adapters and magic state factory modules, and presents a compilation strategy adapted to the constraints of the bicycle architecture. This enables all of the operations we need for universal quantum computing.

The last step is an error correcting decoder, which we will introduce in the Starling proof-of-concept slated for 2028. Alongside our architecture paper, we present the first decoder architecture that is accurate, fast, flexible, and compact. It can fit on an FPGA or ASIC, classical components that are ubiquitous today. This decoding technique, called Relay-BP, achieves a 5x-10x reduction over other leading decoders, and shows that we do not need to use large amounts of HPC to perform the decoding required for fault-tolerant quantum computations.

The IBM roadmap to fault-tolerant quantum computing

Driving our confidence is important theoretical work that demonstrates our ability to hit each of these milestones — and a roadmap to realize it. This year, we've presented an even more detailed version of the IBM Quantum Innovation Roadmap, laying out a timeline to build the critical components required for Starling, introduced in each successive bird.


Innovation Roadmap
IBM Quantum
2016–2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2033+
Software innovation
IBM Quantum Experience
Qiskit
Open-source SDK for building and compiling circuits for quantum hardware
Application modules
Modules for domain specific application and algorithm workflows
Qiskit Runtime
Performance and abstraction through primitives
Quantum Serverless
Demonstrate concepts of managing quantum and cloud classical compute for an end to end workflow
AI-enhanced quantum
Prototype demonstrations of AI-enhanced circuit transpilation
HPC-Quantum integration
Realize an integration of classical HPC and a quantum computer at utility scale
Advantage candidates
Define problem types for advantage in 2026
Error correction decoder
Demonstrate a real-time error correction decoder
Workflow accelerator
Demonstrate a workflow accelerator that streamlines execution for a known advantage workflow
Fault-tolerant ISA
Demonstrate a complete instruction set architecture including magic state distillation for FTQC
Hardware innovation
Early
Canary 5 qubits
Albatross 16 qubits
Penguin 20 qubits
Prototype 53 qubits
Falcon
Demonstrate scaling with I/O routing with bump bonds
Hummingbird
Demonstrate scaling with multiplexing readout
Eagle
Demonstrate scaling with MLW and TSV
Osprey
Enabling scaling with high density signal delivery
Condor
Single-system scaling and fridge capacity
Flamingo
Demonstrate scaling with l-couplers
Loon
Demonstrate c-couplers and next-generation packaging for FTQC
Kookaburra
Demonstrate a complete module consisting of a logical processing unit and quantum memory
Cockatoo
Demonstrate entanglement of modules using a universal adapter
Starling
Demonstrate multiple modules and magic state distillation
Egret
Tunable coupler demonstration
Heron
Architecture based on tunable couplers
Crossbill
Demonstrate m-couplers
Completed
On target

First, the gross code requires more connectivity than our chips currently have — so in 2025, we're building IBM Quantum Loon, a quantum chip with more connectivity and the architecture to enable proof-of-concept experiments toward high-rate qLDPC codes such as these. This includes c-couplers, connectors that can couple qubits more distant than their nearest neighbors.

Then there's the LPU and universal adapters. IBM Quantum Kookaburra, scheduled on our roadmap for 2026, will be the first quantum processor module capable of storing information in a qLDPC memory and processing it with an attached LPU. Meanwhile, IBM Quantum Cockatoo, which sits on our roadmap for 2027, will allow us to demonstrate entanglement between these modules with the universal adapter.

This all comes together with Starling, the system slated for construction in Poughkeepsie, New York. In 2028, Starling will demonstrate the use of magic state injection with multiple modules. In 2029, Starling will scale to a system capable of running one hundred million gates on 200 logical qubits.

Now, while we're confident in our plans to deliver fault-tolerance by 2029, we expect to achieve quantum advantage sooner—by 2026. We've laid out the tools needed to realize and extend quantum advantage with the updated IBM Quantum Development Roadmap, and we are working to ensure that advantages realized before 2029 will run seamlessly on the fault-tolerant quantum computers of 2029 and beyond. Waiting until 2029 to pursue quantum computing could cause companies to fall behind those who start developing advantage-scale applications now.

To accelerate the journey to advantage, we are excited to introduce IBM Quantum Nighthawk, a new processor slated for release later this year. Nighthawk will introduce a 120-qubit square lattice. Much like its predecessor, IBM Quantum Heron, it will be capable of running quantum circuits with 5,000 gates. However, a square lattice enables more qubit connectivity than the heavy hex lattice in Heron. Each qubit in a square lattice is directly connected to four nearest-neighbor qubits, versus two or three in a heavy hex lattice. Higher connectivity will allow Nighthawk to deliver roughly 16x the effective circuit depth of Heron, enabling our clients and users to run much more complex circuits.

We believe Nighthawk will be the platform for exploring the first cases of true quantum advantage, and we will work continuously to improve its quality and connectivity. By 2028, Nighthawk will be able to run circuits with 15,000 gates, and we'll be able to connect up to 9 modules with l-couplers to realize 1,080 connected qubits.

Software is just as important in the journey to advantage. Our updated roadmap uses the Qiskit Runtime engine to improve the scalability of dynamic circuits, and new tools to benchmark use cases and extend them for quantum advantage. It also introduces better error mitigation tools to enable more complex workloads, and utility mapping tools designed to facilitate algorithm discovery for quantum advantage. Other upcoming software advances focus on orchestrating quantum and HPC resources — and we're excited to be introducing a new C API that will allow more direct integrations of Qiskit into HPC environments.

29.Microsoft and Apple Readying Support for Post Quantum Cryptography (PQC) in Next versions of iOS and Windows

by GQI
https://quantumcomputingreport.com/microsoft-and-apple-readying-support-for-post-quantum-cryptography-pqc-in-next-versions-of-ios-and-windows/

At its recent Worldwide Developers Conference (WWDC25), Apple announced that its next major operating system releases for Mac and Windows, iOS 26, iPadOS 26, macOS Tahoe 26, and visionOS 26, will support negotiation of a quantum-secure key exchange algorithm with TLS 1.3 servers that support it. If a server does not yet support one of the quantum-secure exchange algorithms, the operating system will still maintain compatibility and use other key exchange algorithms. The next major operating system releases are expected to be made during Apple's Fall product announcements expected in September. Apple did incorporate support last year for post-quantum cryptography (PQC) in its iMessage app and this next release will expand the support to external servers. You can view Apple's notice about this upcoming support in its next operating system release here.

Microsoft has begun to integrate PQC support into its next version of Windows 11 and it is now available to early users in its Windows Insider program. They will be supporting ML-KEM which is a key encapsulation mechanism based upon the CRYSTALS-Kyber algorithm and also ML-DSA which is a digital signature algorithm based on CRYSTALS-Dilithium algorithm. Although the release date to the general public of this next version of Windows 11 hasn't been determined yet, it is expected later this year. You can view an announcement from Microsoft announcing the availability of PQC to persons participating in the Windows Insider program here and also a previous article we wrote about the company's PQC efforts here.

30. Commvault Unveils New Post-Quantum Cryptography Capabilities to Help Customers Protect Data from a New Generation of Security Threats

https://www.commvault.com/news/commvault-unveils-new-post-quantum-cryptography-capabilities-to-help-customers-protect-data-from-a-new-generation-of-security-threats

At a time when quantum computing is rapidly emerging as an entirely new security challenge for organizations and governments around the world, Commvault, a leading provider of cyber resilience and data protection solutions for the hybrid cloud and one of the first cyber resilience vendors to support post-quantum cryptography (PQC), today announced enhancements to its PQC capabilities. These advancements are designed to help customers protect their highly sensitive, long-term data from a new generation of imminent but unknown cyber threats, creating an additional layer of support, when needed.

Quantum computing uses quantum mechanics to process data and solve complex problems that could take decades with classical computers. However, these advancements bring unprecedented security challenges, along with the potential for threat actors to use quantum computing to decipher and unlock traditional encryption methods. According to the Information Systems Audit and Control Association's (ISACA) Quantum Computing Pulse Poll, 63% of technology and cybersecurity professionals say quantum will increase or shift cybersecurity risks and 50% believe it will present regulatory and compliance challenges1. Now is the time to prepare and take action.

Commvault has provided support for quantum-resistant encryption standards, like CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON, as recommended by the NIST since August 2024. It was then that Commvault introduced a cryptographic agility (crypto-agility) framework, enabling its customers, via the Commvault Cloud platform, to address rapidly evolving threats without overhauling their systems. With today's announcement, Commvault has built on that framework by adding support for Hamming Quasi-Cyclic (HQC), a new error correcting code-based algorithm designed to defend against threats like 'harvest now, decrypt later' where adversaries are intercepting encrypted network traffic and storing it for a later time when quantum computers are powerful enough to decrypt it.

"The quantum threat isn't theoretical," said Bill O'Connell, Chief Security Officer at Commvault. "We were among the first cyber resilience vendors to address post-quantum computing, and by integrating new algorithms like HQC and advancing our crypto-agility framework, we are providing our customers with the tools to navigate this complex landscape with confidence. Our goal is simple and clear: as quantum computing threats emerge, we intend to help our customers keep their data protected."

For industries where long-term data storage is required, like finance and healthcare, Commvault's expanded post-quantum cryptography capabilities provide access to a variety of safeguards that can help fortify network tunnels against quantum-based attacks. With Commvault's Risk Analysis capabilities, customers can discover and classify data to determine where these cryptographic capabilities may be helpful. In addition, Commvault's capabilities are simple to implement, often using a checkbox configuration, making it easy for customers to utilize when needed.

The evolving quantum landscape – the need for speed

As investments pour into the quantum field, the time to address emerging threats is shrinking. This makes proactive adoption of post-quantum cryptography critical.

"Quantum readiness has become a business imperative, particularly for industries which handle data that remains sensitive for decades. The time when currently encrypted data can be decrypted using quantum technology is closer than many people think," said Phil Goodwin, Research VP, IDC. "Commvault's early adoption of quantum-resistant cryptography and commitment to crypto-agility positions it at the forefront among data protection software vendors in proactively addressing quantum threats. Organizations with sensitive, long-term data need to prepare now for a quantum world."

"Commvault has been an invaluable partner in our journey to enhance cyber resilience. Their leadership in adopting post-quantum cryptography, combined with their crypto-agility framework, is exactly what we need to meet stringent government security mandates and protect highly sensitive information from emerging quantum threats," said Jeff Day, Deputy Chief Information Security Officer, Nevada Department of Transportation.

"Safeguarding sensitive data is paramount, and the long-term threat of quantum decryption is a significant concern. Commvault's rapid integration of NIST's quantum-resistant standards, particularly HQC, gives us great confidence that our critical information is protected now and well into the future," said Peter Hands, Chief Information Security Officer, British Medical Association. "Their commitment to crypto-agility is important for healthcare organizations like ours."

Availability

Commvault's post-quantum cryptography capabilities, including support for NIST's HQC algorithm, are immediately available to all Commvault Cloud customers running software version CPR 2024 (11.36) and later, enabling seamless adoption of quantum-resistant protection.

To learn more about Commvault's quantum-resistant encryption solutions and how to future-proof your data security strategy, read today's blog, watch our executive videos here and here, and check out the executive brief.

31. Our Online World Relies on Encryption. What Happens If It Fails?

by Maureen Stanton
https://www.bu.edu/articles/2025/our-online-world-relies-on-encryption-what-happens-if-it-fails/

In our hyper-connected world, we rely on encrypted communications every day — to shop online, digitally sign documents, make bank transactions, check our steps on fitness trackers.

But today's encryption, which transforms data into unreadable formats to keep our information secure, is under intense pressure. Cybercriminals are increasingly sophisticated, and our networks – woven with cloud services and third-party platforms – are more vulnerable than ever. JP Morgan reports it repels 45 billion hacking attempts *a day*.

The most significant threat is something called Y2Q or Q-Day: the date quantum computers will make most current encryption methods obsolete. To grasp the scale, a quantum computer could do in a day what the world's current fastest supercomputer would need millennia to accomplish: break RSA-2048 encryption, an algorithm that's the backbone of internet security. It's not an overstatement to say that, without encryption, the entire security of our connected world would collapse, threatening the stability of society. While Y2Q may be years away, there is also a growing need to boost the resilience of encryption. "Harvest now, decrypt later" attacks are escalating—a strategy where cybercriminals harvest encrypted data today with the intent of decrypting it later when quantum tools become available.

To address these challenges, a Boston University–led multidisciplinary research team, supported by a $3.6 million National Science Foundation (NSF) Growing Convergence Research award, is developing a groundbreaking, physics-inspired approach to data security and privacy. Their method reimagines the very foundations of encryption tools and they say it promises to be more robust, scalable, and future-ready in the face of rapidly evolving cyber threats. The team, which includes collaborators at Cornell University and the University of Central Florida, has just published a paper in the *Proceedings of the National Academy of Sciences (PNAS)* that illustrates some of the ideas driving its approach to cryptography.

"We're in a new era of technology, where the frontiers of computational capability lie at the intersection of classical and quantum computing, AI, and data security," says principal investigator Andrei Ruckenstein, a BU College of Arts & Sciences Distinguished Professor of Physics. "The most urgent and complex challenges in these areas, such as safeguarding sensitive data or preparing for the quantum threat, cannot be solved by current encryption and security methods. What's exciting about this work is that it introduces a true paradigm shift and provides new capabilities made possible only through diverse disciplines forging a fundamental change in thinking."

Quantum computing taps into unusual properties of the very small—where particles can exist in multiple states simultaneously (quantum superposition) and stay connected over distance (entanglement), allowing a quantum computer to explore many possibilities at once, significantly speeding up certain computations.

"Our approach is expected to be inherently resistant to both classical and quantum attacks," says Ruckenstein. "It would not only strengthen public confidence in AI systems, but also unlock new opportunities for data-powered, socially responsible innovation."

Protecting Data During Use

Modern encryption methods, developed roughly 50 years ago, could not envision the computational demands of today – let alone those of the quantum era. Relying on hard-to-solve mathematical problems, these systems mostly only protect data in transit or at rest—leaving it exposed during use. That poses a problem for data-intensive applications like AI training models, which process vast amounts of data that is often private or confidential. Current approaches typically require models to decrypt data during training, leaving it exposed, or employ privacy-preserving techniques that slow processing speeds, making them difficult to apply at scale.

The BU-led NSF project offers a new path forward. The proposed scheme, called Encrypted Operator Computing (EOC), merges physics, computer science, and mathematics to develop scalable methods for computing directly on encrypted data — long considered the “holy grail” of cryptography.

“The approach is an alternative to Fully Homomorphic Encryption (FHE), an elegant, state-of-the-art cryptographic tool, which has so far proven difficult to apply to large-scale practical problems,” says Ruckenstein.

The EOC allows users to manipulate and gain insights from confidential data without ever exposing the raw information to third parties. This level of security and privacy is essential for applications such as blockchain transactions, medical AI models, cloud services, and more.

“While our EOC method is designed to work on classical computers doing classical computations, the conceptual breakthrough behind it is quantum computation–inspired,” says Claudio Chamon, a CAS professor of physics. “In addressing the real-world challenge of computation on encrypted data, we also encounter fundamental questions, such as how many distinct ways a given computation can be expressed for a fixed-length circuit. We relate these questions to thermodynamic concepts like ‘entropy,’ which describes how unpredictable or random a system is based on how many ways it can be arranged.”

How entropy applies to computation is the subject of the team’s *PNAS* paper. “In our framework, computation is represented as a circuit of logical elements, or gates, encoding elementary operations and which, when applied sequentially to the input data, implement the desired computation,” says Ruckenstein, who co-authored the paper with Chamon, Ran Canetti, a CAS professor of computer science, and Eduardo R. Mucciolo, a professor of physics at the University of Central Florida. “In the paper, we considered both the functionality and complexity of computational circuits — what the circuit is computing and how large a circuit is needed to implement that computation.”

The team’s physics-inspired approach treats complexity in computing as a thermodynamic quantity; thermodynamics relates to how things like heat and energy spread. The rules of thermodynamics govern how, for example, the heat diffuses in your morning coffee: as the heat spreads, the molecules become more distributed and disordered, their patterns more complex. None of which stops you from enjoying your coffee—but good luck recovering the history of all those erratic molecules. The researchers suggest that, in a computer circuit, its gates can similarly be disordered to hide information.

The *PNAS* paper proposes a dynamic process to obfuscate, or “hide,” any circuit by rearranging gates, randomizing its structure without altering its function. The aim is to not only scramble information fast, but also do so thoroughly—essentially destroying all patterns, so that a program is impossible to reverse engineer. The team’s vision is to create a trustworthy environment where both the data and programs that use the data stay hidden.

“Program obfuscation is an extremely powerful and versatile concept for protecting data, its processing, and its various uses in multiple scenarios and over time,” says Canetti. “However, it is notoriously hard to construct: to date, we have no general-purpose program obfuscation scheme that is even close to being practical. This exciting project has the potential to make program obfuscation a reality.”

Breaking Boundaries Through Convergent Research

The NSF-funded project aims to turn these cryptography concepts into practical tools. Together, the research team will develop the EOC framework into scalable, special-purpose hardware, merging physics-inspired insights about information with advanced cryptography and pure mathematics. The goal is to accelerate performance and make secure, privacy-preserving computing widely accessible for real-world use.

“By combining expertise from diverse areas, we can tackle problems from multiple angles at once—whether it’s understanding quantum behavior, designing new algorithms, or building better hardware,” says Mucciolo. “This synergy not only speeds things up, but also allows us to dive much deeper than any one discipline could alone. We’re uncovering connections that wouldn’t be visible without this kind of cross-disciplinary perspective.”

One of the team’s other contributors, Timothy Riley, a professor of mathematics at Cornell University, says the collaboration across disciplines is a “rare and precious opportunity” that is allowing the researchers “to understand each other’s languages, to learn from each other’s perspectives, and to share the models, problems, and abstractions that drive our work.”

Canetti, Chamon, and Ruckenstein were able to advance the work with the support of the Hariri Institute’s Quantum Convergence Focused Research Program, which facilitates convergent thinking and multidisciplinary collaborations across BU on cross-cutting themes around quantum science and engineering. All three BU researchers are affiliated with the institute.

“The rise of digital infrastructure demands stronger security to protect our economy, privacy, and national interests,” says Yannis Paschalidis, a BU College of Engineering Distinguished Professor of Engineering, director of the Hariri Institute, and a member of the University’s Task Force on Convergent Research and Education. “Solving these complex challenges requires breaking down silos. This work shows how convergent research can drive real-world impact and unlock entirely new technological frontiers.”