Crypto News

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

November 04, 2024

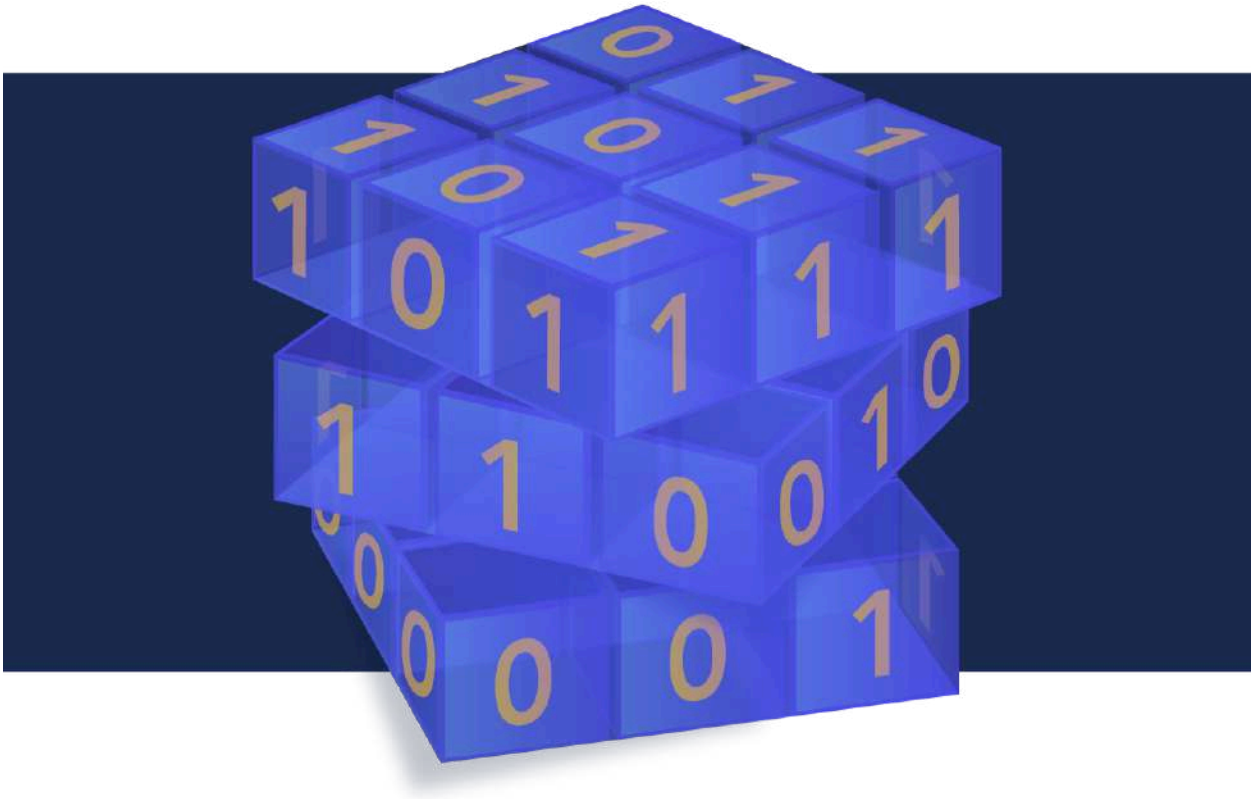


Table of Contents

Table of Contents **2**
Editorial **4**
1. Here's the paper no one read before declaring the demise of modern cryptography 5
2. Samsung Sets New Benchmark in TV Security With FIPS 140-3 Certification 10
3. Secure-IC obtains the first worldwide CAVP Certification of Post-Quantum Cryptography algorithms, tested by SERMA Safety & Security 11
4. Cybersecurity Awareness Month 2024 11
5. 'The Splurge' to seek better cryptography to prepare for quantum computers: Buterin 13
6. 'The Splurge' to seek better cryptography to prepare for quantum computers: Buterin 15
7. Post-Quantum Cryptography Market Forecast 2031|ID Quantique, SeQureNet, Quintessence Labs, MagiQ Technologies 17
8. Round 2 PQC Additional Signatures: Multivariate and MPC-in-the-Head To The Fore 20
9. Can this cryptography tool secure your supply chain data? 23
10. Quantum computer 'threat' to crypto is exaggerated — for now 26
11. Why IT Leaders are Fast-Tracking Post-Quantum Cryptography 31
12. Are WhatsApp and Signal Secure Enough for Confidential or Secret Communications? 33
13. WeChat devs introduced security flaws when they modded TLS, say researchers 35
14. Post-Quantum Cryptology: How Secure Memory Can Protect Against Vulnerabilities 37
15. Tiny Computer, Big Advance: Taiwan Develops Small Quantum Computer Using Single Photon 39
16. Debunking Hype: China Hasn't Broken Military Encryption With Quantum 40
17. A Blueprint for Canadian Deep Tech Leadership from Quantum Industry Canada 43
18. Most Organizations Unprepared for Post-Quantum Threat 56
19. Google's 67-Qubit Sycamore Quantum Computer Could Beat Top Supercomputers: Study 57
20. Canada's Quantum Leap: A Call to G7 Leadership 59
21. NATO's Quantum-Safe Future Transition 60
22. Chinese Scientists Report Using Quantum Computer to Hack Military-grade Encryption 61
23. Encryption backdoor debates rage across the planet, promising a difficult 2025 for CISOs 63
24. A New Phase for Quantum Competition in Europe 66
25. Research team develops hardware architecture for post-quantum cryptography 68
26. IonQ Demonstrates Remote Ion-Ion Entanglement, a Significant Milestone in Developing Networked Quantum Systems at Scale 71
27. D-Wave Introduces Service-Level Agreements for Leap Quantum Cloud Customers in

Production 72
28. What Communications Companies Need to Know Before Q-Day 73
29. How post-quantum cryptography is reshaping cybersecurity in 2024 75
30. CISA aims for inventory clarity with post-quantum cryptography guidance 76
31. IBM algorithms chosen as part of NIST's first post-quantum standards 77
32. First IBM Quantum Data Center in Europe Opens 78
33. NordVPN Launches Post-quantum Encryption Support for First Application 81

Editorial

Hello Readers! I'm back and excited to share everything quantum newsworthy with you this month. This is a particularly exciting newsletter since it highlights a nation-state who reported having created a quantum computer that could break military grade encryption while other articles simultaneously de-bunking the claim. You'll want to start with article 22 to refresh your memory about the claims made back in May that a nation-state had used a quantum computer to hack military grade encryption. Then you'll want to scroll back up to articles 1 and 16 to get the real story. What a whirlwind!

I'll admit, the nation-state made progress and took an incremental step, however, it was not a breakthrough. The work completed was with a quantum annealer which isn't often capable of executing an algorithm like Shor's algorithm. It is noteworthy that researchers are working to see if quantum annealers could be used to execute powerful algorithms in the near future. The paper claimed it attacked RSA encryption, however, RSA is not considered military grade. What researchers did do is factor a 50-bit integer which is quite an achievement, however, nowhere near the 2048 bit keys and larger that RSA utilizes. Going from 50 bits to 2048 doesn't mean that the problem is only 40 times harder to solve but exponentially more difficult. The unfolding of this saga reminds us to stay vigilant and continue to ask intelligent and fact-based questions when we hear claims of a breakthrough showcasing a quantum-advantage.

Do keep in mind that a quantum-advantage is still on the horizon and organizations and governments alike need to be prepared. If you're looking into how to do so, make your way to article 5 for some high-level steps on how to be crypto-agile which is a step in the right direction. Another great article is article 19 which is yet another incremental step in the direction of seeing a true quantum-advantage. Get an overview of Google's 67-Qubit Sycamore Quantum Computer and then dive into Google's claims that "the Sycamore chip is capable of executing calculations that exceed the performance capabilities of traditional supercomputers." This is truly an exciting newsletter that you'll want to read cover-to-cover. Until next time readers!

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

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

1. Here's the paper no one read before declaring the demise of modern cryptography

by Dan Goodin
https://arstechnica.com/information-technology/2024/10/the-sad-bizarre-tale-of-hype-fueling-fears-that-modern-cryptography-is-dead/

There's little doubt that some of the most important pillars of modern cryptography will tumble spectacularly once quantum computing, now in its infancy, matures sufficiently. Some experts say that could be in the next couple decades. Others say it could take longer. No one knows.

The uncertainty leaves a giant vacuum that can be filled with alarmist pronouncements that the world is close to seeing the downfall of cryptography as we know it. The false pronouncements can take on a life of their own as they're repeated by marketers looking to peddle post-quantum cryptography snake oil and journalists tricked into thinking the findings are real. And a new episode of exaggerated research has been playing out for the past few weeks.

All aboard the PQC hype train

The last time the PQC—short for post-quantum cryptography—hype train gained this much traction was in early 2023, when scientists presented findings that claimed, at long last, to put the quantum-enabled cracking of the widely used RSA encryption scheme within reach. The claims were repeated over and over, just as claims about research released in September have for the past three weeks.

A few weeks after the 2023 paper came to light, a more mundane truth emerged that had escaped the notice of all those claiming the research represented the imminent demise of RSA—the research relied on Schnorr's algorithm (not to be confused with Shor's algorithm). The algorithm, based on the 2021 analysis of cryptographer Peter Schnorr, had been widely debunked two years earlier. Specifically, critics said, there was no evidence supporting the authors' claims of Schnorr's algorithm achieving polynomial time, as opposed to the glacial pace of subexponential time achieved with classical algorithms.

Once it became well-known that the validity of the 2023 paper rested solely on Schnorr's algorithm, that research was also debunked.

Three weeks ago, panic erupted again when the South China Morning Post reported that scientists in that country had discovered a "breakthrough" in quantum computing attacks that posed a "real and substantial threat" to "military-grade encryption." The news outlet quoted paper co-author Wang Chao of Shanghai University as saying, "This is the first time that a real quantum computer has posed a real and substantial threat to multiple full-scale SPN [substitution–permutation networks] structured algorithms in use today."

Among the many problems with the article was its failure to link to the paper—reportedly published in September in the Chinese-language academic publication Chinese Journal of Computers—at all. Citing Wang, the paper said that the paper wasn't being published for the time being "due to the sensitivity of the topic." Since then, the South China Morning Post article has been quietly revised to remove the "military-grade encryption" reference.

With no original paper to reference, many news outlets searched the Chinese Journal of Computers for similar research and came up with this paper. It wasn't published in September, as the news article reported, but it was written by the same researchers and referenced the "D-Wave Advantage"—a type of quantum computer sold by Canada-based D-Wave Quantum Systems—in the title.

Some of the follow-on articles bought the misinformation hook, line, and sinker, repeating incorrectly that the fall of RSA was upon us. People got that idea because the May paper claimed to have used a D-Wave system to factor a 50-bit RSA integer. Other publications correctly debunked the claims in the South China Morning Post but mistakenly cited the May paper and noted the inconsistencies between what it claimed and what the news outlet reported.

Over the weekend, someone unearthed the correct paper, which, as it turns out, had been available on the Chinese Journal of Computers website the whole time. Most of the paper is written in Chinese. This abstract was fortunately written in English. It reports using a D-Wave-enabled quantum annealer to find "integral distinguishers up to 9-rounds" in the encryption algorithms known as PRESENT, GIFT-64, and RECTANGLE. All three are symmetric encryption algorithms built on a SPN—short for substitution-permutation network structure.

"This marks the first practical attack on multiple full-scale SPN structure symmetric cipher algorithms using a real quantum computer," the paper states. "Additionally, this is the first instance where quantum computing attacks on multiple SPN structure symmetric cipher algorithms have achieved the performance of the traditional mathematical methods."

Defining your terms

There's a lot going on here, but what does it mean? To explain, here's a quick explanation of several important terms.

SPN: Short for substitution-permutation network, an SPN is a series of mathematical operations used in block cipher algorithms to increase their security. These algorithms take a block of plaintext and the encryption key as input and run them through a subprocess that repeats for a set number of rounds before outputting a finished ciphertext.

The best known block cipher is AES, short for Advanced Encryption Standard. Ciphertext produced with 128-bit, 192-bit, and 256-bit AES go through 10 rounds, 12 rounds, and 14 rounds respectively. Page 5 of this animation tutorial provides a useful visualization of this process.

Quantum annealing: This term is borrowed from annealing, a process that uses heat to alter the physical or chemical properties of a metal, glass, or plastic film to increase ductility and reduce hardness. Annealing works by heating materials above their recrystallization temperature, maintaining a certain temperature for a set amount of time, and then allowing them to cool slowly.

The "annealing" in quantum annealing is used metaphorically to describe a method for applying the principles of quantum mechanics to solve complex optimization problems. More on quantum annealing here and here.

In 2011, D-Wave produced the first commercial quantum annealer. Called the D-Wave One, it used a 128-qubit processor chipset. The D-Wave Advantage, the system used in the September research paper, has 5,000 qubits. D-Wave systems can solve only certain types of optimization problems, and the difficulty requires developers and scientists using D-Wave systems to break larger problems into smaller optimization problems before they can be solved with these systems.

PRESENT, GIFT64, and RECTANGLE: All three are lightweight block ciphers designed for use in "constrained" environments, such as those in embedded systems that require more speed and fewer computational resources than is possible using AES. All three are based on an SPN structure and are proposed academic designs. The related GIFT-128 is a component of GIFT-COFB, which was a finalist for the recent NIST lightweight crypto competition but lost out to an algorithm known as Ascon.

PRESENT, meanwhile, can be found in the ISO/IEC 29167-11:2014 and ISO/IEC 29192-2:2019, but it isn't used widely. It's not clear if RECTANGLE is used at all. Because all three algorithms were academic designs, they have been widely analyzed.

Integral distinguishers: In essence, finding integral distinguishers is a type of large-scale optimization problem that, when solved, provides a powerful tool for breaking encryption schemes used in block ciphers. A 2018 paper titled *Finding Integral Distinguishers with Ease* reported using classical computing to find integral distinguishers for dozens of algorithms. The research included 9-round distinguishers for PRESENT, GIFT64, and RECTANGLE, the algorithms studied in the September paper.

Mixed-integer linear programming: Typically abbreviated as MILP, mixed-integer linear programming is a mathematical modeling technique for solving complex problems. MILP allows some variables to be non-integers, a property that gives it flexibility, efficiency, and optimization over other methods.

The experts weigh in

The main contribution in the September paper is the process the researchers used to find integral distinguishers in up to nine rounds of the three previously mentioned algorithms. According to a roughly translated version of the paper (the correct one, not the one from May), the researchers wrote:

> *Inspired by traditional cryptanalysis methods, we proposed a novel computational architecture for symmetric cryptanalysis: Quantum Annealing-Classical Mixed Cryptanalysis (QuCMC), which combines the quantum annealing algorithm with traditional mathematical methods. Utilizing this architecture, we initially applied the division property to describe the propagation rules of the linear and nonlinear layers in SPN structure symmetric cipher algorithms.*
>
> *Subsequently, the SPN structure distinguisher search problems were transformed into Mixed Integer Linear Programming (MILP) problems. These MILP models were further converted into D-Wave Constrained Quadratic Models (CQM), leveraging the quantum tunneling effect induced by quantum fluctuations to escape local minima solutions and achieve an optimal solution corresponding to the integral distinguisher for the cipher algorithms being attacked. Experiments conducted using the D-Wave Advantage quantum computer have successfully executed attacks on three representative SPN structure algorithms: PRESENT, GIFT-64, and RECTANGLE, and successfully searched integral distinguishers up to 9-round. Experimental results demonstrate that the quantum annealing algorithm surpasses traditional heuristic-based global optimization algorithms, such as simulated annealing, in its ability to escape local minima and in solution time. This marks the first practical attack on multiple full-scale SPN structure symmetric cipher algorithms using a real quantum computer.*
>
> *Additionally, this is the first instance where quantum computing attacks on multiple SPN structure symmetric cipher algorithms have achieved the performance of the traditional mathematical methods.*

The paper makes no reference to AES or RSA and never claims to break anything. Instead, it describes a way to use D-Wave-enabled quantum annealing to find the integral distinguisher. Classical attacks have had the optimized capability to find the same integral distinguishers for years. David Jao, a professor specializing in PQC at the University of Waterloo in Canada, likened the research to finding a new lock-picking technique. The end result is the same, but the method is new. He explained:

> *The paper is written for an audience of researchers, not for the general public. Researchers view "developing a better lockpick" as an actual attack, but if you're writing for the general public, the general public would think that an attack means "using the lockpick to pick the lock" which is not what happened here.*
>
> *To continue the analogy, it's true that this paper uses quantum computers to develop lockpicks that match previously known lockpicks in efficiency. So it is true that they have "achieved the performance" of traditional methods, although note that they have not gone beyond that. In some cases (such as RECTANGLE), it is known that no better integral distinguishers exist, so matching the existing technology is the best that can be done using this approach.*

Nadia Heninger, a professor studying cryptography at the University of California San Diego, agreed.

"I'd say it's more accurate to say that the researchers formulated a cryptanalysis problem as an optimization problem and ran it on simulated annealing and on quantum annealing and claim to have gotten comparable

results. But the main result is to have 'achieved the performance of traditional mathematical methods,' so it sounds like maybe there are other classical/mathematical approaches that are better."

Lastly, Xavier Bonnetain, a researcher at the National Institute for Research in Digital Science and Technology in France, put it this way:

> *They claimed they reduced the search for what is called an integral distinguisher to a Mixed-Integer Linear Programming problem (something that's been standard for years in cryptography) and solved the problem for 3 block ciphers using their quantum annealer.*
>
> *They did not find anything new, which is not especially surprising given that integral distinguishers on these ciphers were already looked for classically and were already proven optimal. They solved a problem for which we already knew the answers, using another approach.*

After performing a quick search, Bonnetain found this 2018 paper that found integral distinguishers for all three of the algorithms covered in the September paper.

None of these experts are denigrating the research presented in the September paper. They are, however, noting that the claims presented in the original South China Morning Post article—and repeated in the ensuing media echo chamber afterward—go beyond mere exaggeration or embellishment. Instead, they're more comparable to fabrications. Even many of the articles debunking the claims—while well intentioned—missed the mark because they, too, cited the wrong paper.

This isn't the first time the South China Morning Post has fueled undue panic about the imminent fall of widely used encryption algorithms. Last year's hype train, mentioned earlier in this article, was touched off by coverage by the same publication that claimed researchers found a factorization method that could break a 2,048-bit RSA key using a quantum system with just 372 qubits. People who follow PQC should be especially wary when seeking news there.

The coverage of the September paper is especially overblown because symmetric encryption, unlike RSA and other asymmetric siblings, is widely believed to be safe from quantum computing, as long as bit sizes are sufficient. PQC experts are confident that AES-256 will resist all known quantum attacks.

I emailed two of the co-authors of the September paper: Wang Chao, mentioned earlier, and Pei Zhi, a PhD. candidate at Shanghai University, asking for their help with this story. The only response I got was two auto-replies saying their inboxes were full.

As a reminder, current estimates are that quantum cracking of a single 2048-bit RSA key would require a computer with 20 million qubits running in superposition for about eight hours. For context, quantum computers maxed out at 433 qubits in 2022 and 1,000 qubits last year. (A qubit is a basic unit of quantum computing, analogous to the binary bit in classical computing. Comparisons between qubits in true quantum systems and quantum annealers aren't uniform.) So even when quantum computing matures

sufficiently to break vulnerable algorithms, it could take decades or longer before the majority of keys are cracked.

The upshot of this latest episode is that while quantum computing will almost undoubtedly topple many of the most widely used forms of encryption used today, that calamitous event won't happen anytime soon. It's important that industries and researchers move swiftly to devise quantum-resistant algorithms and implement them widely. At the same time, people should take steps not to get steamrolled by the PQC hype train.

2. Samsung Sets New Benchmark in TV Security With FIPS 140-3 Certification

https://news.samsung.com/global/samsung-sets-new-benchmark-in-tv-security-with-fips-140-3-certification

Samsung Electronics today announced that its proprietary cryptography module, Samsung CryptoCore[1], has earned the prestigious FIPS 140-3 certification[2] from the National Institute of Standards and Technology (NIST). This certification underscores Samsung's commitment to providing industry-leading security and data protection for Smart TV users.

"As home entertainment systems become more connected, it becomes critical for technology companies to safeguard the personal data that enables the seamless connectivity enjoyed by so many," said Yongjae Kim, Executive Vice President and Head of the R&D Team, Visual Display Business at Samsung Electronics. "By integrating the FIPS 140-3-certified CryptoCore into our Smart TVs, Samsung is taking our commitment to secure home entertainment a step further and ensuring that our users can freely experience the value of our products."

Beginning in 2025, Samsung CryptoCore will be fully integrated into Tizen OS[3], Samsung's Smart TV operating system, enhancing the security of key products such as TVs, monitors and digital signage. With Samsung CryptoCore embedded in Tizen OS, personal data linked to Samsung accounts will be securely encrypted, SmartThings authentication information will be protected from external hacking threats and content viewed on TVs will benefit from enhanced copyright protection.

Since 2015, Samsung has equipped its Smart TVs with Samsung Knox[4], a security platform that has earned Common Criteria (CC) certification[5] for 10 consecutive years. But with its newly acquired FIPS 140-3

[1] *Samsung CryptoCore is a software library that encrypts and decrypts data during both transmission and storage.*

[2] *Federal Information Processing Standard (FIPS) 140-3 covers the security requirements for cryptographic modules.*

[3] *Tizen OS 9.0.*

[4] *Samsung Knox provides privacy protection on its Smart TVs through features like Tizen OS Monitoring, Phishing Site Blocking and Knox Vault. Knox Vault is available only on the QN900D and QN800D models.*

[5] *Common Criteria (CC) certification is a global security standard recognized by 31 countries for IT product integrity.*

certification, Samsung has strengthened its defenses against hacking and data breaches even further, proactively protecting personal information with advanced encryption technology.

Recognized by governments in 10 countries[6], the FIPS 140-3 certification requires comprehensive testing of cryptographic modules to ensure their security, integrity and reliability. For users, this means Samsung Smart TVs offer cutting-edge protection against privacy breaches, allowing them to enjoy their content, connect smart devices and engage with IoT services securely and without concerns.

3. Secure-IC obtains the first worldwide CAVP Certification of Post-Quantum Cryptography algorithms, tested by SERMA Safety & Security

https://www.design-reuse.com/news/56991/secure-ic-cavp-certification-of-post-quantum-cryptography-algorithms-serma-safety-security.html

Secure-IC, the rising leader, and global provider of end-to-end cybersecurity solutions for embedded systems and connected objects, has achieved a historical milestone by becoming the first security IP and software vendor worldwide to receive CAVP (Cryptographic Algorithm Validation Program) Hardware certification for its Post-Quantum Cryptography (PQC) algorithms. This groundbreaking certification has been conducted by SERMA Safety & Security, a globally recognized leader in security evaluation.

Secure-IC PQC solutions, fully already integrated into the recently launched Securyzr™ neo product range, have successfully passed rigorous testing and evaluation based on the newly established standards set forth last summer by the National Institute of Standards and Technology (NIST). This certification covers the critical algorithms ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism, originally known as CRYSTALS-Kyber), ML-DSA (Module-Lattice-Based Digital Signature Standard, originally CRYSTALS-Dilithium) and more upcoming, ensuring these technologies are designed in line with the NIST standards (namely FIPS 203, FIPS 204), developed to resist the quantum computing threats of the future. Secure-IC's PQC implementations were tested within the frame of a Securyzr™ Crypto Solutions/Crypto-coprocessors neo product, that can be seamlessly integrated within our Securyzr™ iSE neo product range. The official certificate (A6046) can be found on the NIST website.

4. Cybersecurity Awareness Month 2024

by Amy Mahn

https://www.nist.gov/blogs/cybersecurity-insights/staff-stories-spotlight-series-cybersecurity-awareness-month-2024

[6] *Recognized in the United States, Canada, UK, Germany, France, South Korea, Japan, Singapore, Australia and New Zealand.*

This year's Cybersecurity Awareness Month theme is 'Secure our World.' How does this theme resonate with you, as someone working in cybersecurity?

This theme resonates strongly with me. I am very fortunate to have the role of leading and supporting international engagement on cybersecurity and privacy resources in the Applied Cybersecurity Division at NIST. The theme to "secure our world" as an imperative reflects the importance of international engagement and working with stakeholders throughout the world on shared objectives like managing cybersecurity risks. This includes the development of cybersecurity and privacy resources, and at NIST, we develop and update our guidance with through close collaboration with partners around the world. We obtain extensive stakeholder feedback and are mindful of global approaches and policies to help our resources be internationally accessible. Through our valuable international engagements and collaborations, we can continue to develop and share these resources and contribute along with our partners to improving cybersecurity risk management practices throughout the world.

Describe your career pathway and how that led you to the cybersecurity field?

During my college years, I completed a semester in Washington, D.C. that included an internship on Capitol Hill. Following that semester, I returned to the D.C. area and began a graduate program at American University. I also worked at the Department of Homeland Security (DHS) for several years, and while at DHS I developed an interest in cybersecurity work as well as international engagement. I learned more about the mission and cybersecurity efforts of NIST through a detail assignment, and after DHS I began work in the Applied Cybersecurity Division at NIST. In this current role, I have had the opportunity to work on international engagement on cybersecurity and privacy resources. My various roles at DHS and now at NIST gave me an excellent opportunity to learn from leadership and colleagues at these offices about cybersecurity risk management, especially from the international perspective.

Describe the role(s) that you play at NIST. What are some interesting projects you've worked on recently?

I lead and support international engagement on cybersecurity and privacy resources in the Applied Cybersecurity Division in the Information Technology Laboratory at NIST. I work with colleagues across NIST to advance our international engagement on resources such as the Cybersecurity Framework. I also help ensure that NIST resources continued to be used and of value to government, industry, and academia throughout the world. I represent NIST at international cybersecurity dialogues led by the State Department and International Trade Administration (ITA) to help ensure NIST equities are represented and strengthen our collaboration and engagement with international governments. I also coordinate engagement with industry on international engagement and regularly represent NIST to speak at events on our work and international engagement. I help coordinate and facilitate meetings for international partners who visit NIST and our National Cybersecurity Center of Excellence (NCCoE), where we collaborate with industry to develop cybersecurity solutions. I support standards development efforts around NIST cybersecurity and privacy resources. I have participated in efforts at ISO (International Organization for Standardization) to contribute to and help with the development of ISO documents that use and references resources like the NIST Cybersecurity Framework (CSF).

The recent update of the NIST CSF to version 2.0 has presented exciting opportunities for continued international engagement. Recently, I participated in a workshop in Mexico City that NIST collaborated with the International Trade Administration and Department of State to develop, and I had the chance to present to and speak with Mexican government and industry about the CSF 2.0. I continue to present virtually and in person on the CSF and other NIST cybersecurity and privacy resources with international partners and highlight opportunities to collaborate and engage. I help with international translations of NIST resources which can be found on the NIST International Cybersecurity and Privacy Resources site. These translations include those done directly by NIST or the US government and translations we have verified from individuals who share them with us as a resource. The page of current translations we are aware of can be found here. I also share information about the important international engagement efforts of our NIST team through a Taking Measure blog. I continue to update it to show the valuable conversations and events NIST is participating in with government and industry throughout the world in an effort to make our work more globally accessible.

What is your favorite part about working at NIST?

There are many reasons to enjoy working at NIST. The working environment at NIST really fosters creativity and innovation, and employees are given many opportunities to learn and develop professionally within their roles. I have learned so much from my colleagues and benefit every day from their expertise and guidance. I have felt greatly supported by my team to continue growing our international footprint, and I appreciate how willing everyone is to support our international engagements and share information with our partners. I feel fortunate to work with dedicated and hard-working colleagues at NIST who focus on their mission as well as the people working to achieve it.

5. 'The Splurge' to seek better cryptography to prepare for quantum computers: Buterin

by Amy Larsen DeCarlo
https://www.techtarget.com/searchsecurity/tip/How-to-achieve-crypto-agility-and-future-proof-security

Quantum computing promises organizations the ability to optimize processes, overcome logistical challenges, reduce costs and improve decision-making. Quantum computing's advanced functionality and compute capabilities, however, also mean current cryptographic algorithms will no longer provide the protection they once did.

While the quantum computing market is still nascent, with revenue estimates for 2024 around $1.3 billion, it is expected to grow to $5.3 billion by 2029. With current asymmetric encryption at risk, it's critical that organizations prepare now for post-quantum cryptography (PQC) -- a key aspect of which is adopting crypto-agility.

What is crypto-agility and why is it important?

Crypto-agility is an approach that enables systems to dynamically shift among multiple cryptographic algorithms, mechanisms and key management systems as needed to counter threats. It applies changes without interrupting the system's infrastructure. This approach is both a proactive defensive measure and an incident response tool that is used when a cryptographic algorithm is found to be compromised.

A successful crypto-agile system is one where the algorithms can be switched out with ease and at least partially through automation. The goal of agile cryptography management is to enable organizations to future-proof systems' abilities to counter threats to cryptography.

Steps to achieve crypto-agility

The best way to overcome post-quantum security challenges is to have a solid implementation plan, which should include the following:

1. **Create crypto-agile policies and processes.** Create and implement policies and processes for shifting between algorithms if they become compromised. Automate these processes where possible.

2. **Develop communication and incident response plans.** All organizational staff need to understand their individual roles in executing crypto-agile policies and keeping stakeholders apprised of changes. Also, train employees on any new tools and processes, as well as how to recognize and respond to post-quantum threats that might arise.

3. **Conduct a cryptographic asset inventory.** Keep an inventory of cryptographic algorithms, digital certificates and key management systems to understand the full scope of PQC migration and to determine where to implement PQC algorithms first. Review regularly to keep the inventory up to date.

4. **Deploy a key management system.** Cryptographic keys need to be managed, updated and rotated on a consistent basis. Key management systems help automatically create, store and alternate cryptographic keys.

5. **Implement a public key infrastructure for PQC.** Use PKI to automatically create, distribute, manage, maintain, and replace keys and digital certificates.

6. **Consider legacy systems.** Avoid potential issues by creating a pragmatic migration plan for nonagile systems. First, determine which systems and applications can be updated, and then discern how to update and secure them. Be sure to budget for costs associated with transitioning to PQC.

7. **Perform rigorous systems testing and ongoing validation.** Test and audit quantum security controls and processes to detect and remediate weaknesses and vulnerabilities. Also, consider backups and recovery strategies.

8. **Prepare for future threats with quantum computing.** Quantum computing can help elevate an organization's security posture. For example, consider quantum machine learning, which will be able to expedite threat identification and detect attacks before they penetrate a network.

6. 'The Splurge' to seek better cryptography to prepare for quantum computers: Buterin

by JESSE COGHLAN
https://cointelegraph.com/news/vitalik-buterin-the-splurge-advanced-cryptography-plan-for-quantum-computers

Ethereum co-founder Vitalik Buterin said one of the blockchain's roadmap stages aims to research "advanced cryptography," to make it resistant to future quantum computers that can break encryption.

"There is a heck of a lot left to do," Buterin wrote in an Oct. 29 blog post, which shared his thoughts on a part of the blockchain's roadmap dubbed "The Splurge."

Still, he said that quantum computers – which would be powerful enough to break encryption – "do not even exist."

Buterin added any purported quantum computer currently touted on the internet "are either prototypes" or are just "not real quantum computers, in the sense that while they may have quantum parts in them, they cannot actually run meaningful computations."

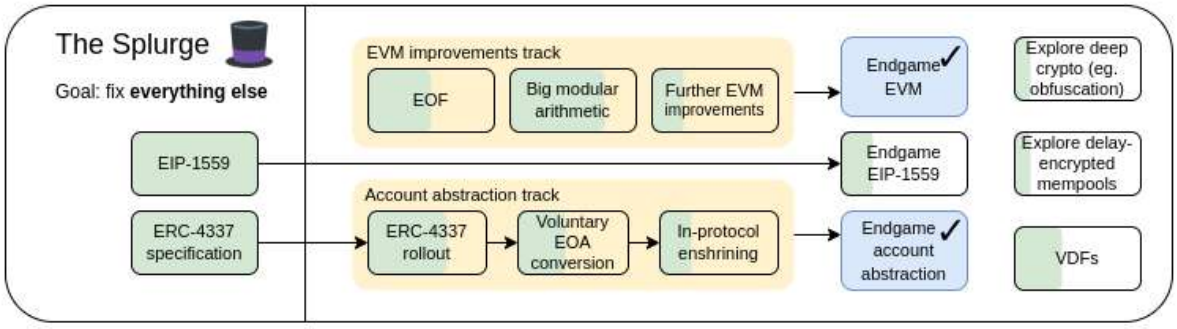
"Even if 'real' quantum computers come soon, the day when regular people have quantum computers on their laptops or phones may well be decades after the day when powerful institutions get one that can crack elliptic curve cryptography."

The Ethereum co-founder's thoughts were shared in the post on his plan for The Splurge, the sixth in a series of ideas he's shared on Ethereum's roadmap, with this stage aiming to "fix everything else" with the blockchain.

Each stage – including The Merge, The Surge, The Scourge, The Verge and The Purge – happens concurrently and focuses on different aspects of the blockchain.

Buterin said The Splurge largely focuses on Ethereum Virtual Machine (EVM) improvements and "various niche topics."

"There are lots of 'little things' in Ethereum protocol design that are very valuable for Ethereum's success, but don't fit nicely into a larger sub-category," he said. "This is what 'the Splurge' is for."



A diagram showing The Splurge portion of Ethereum's roadmap. Source: Vitalik Buterin

He added that The Splurge's key goals are to bring the EVM to a "stable 'endgame state,'" bring account abstraction in-protocol and optimize the economics of transaction fees alongside looking into "advanced cryptography."

Ethereum's next update, called Pectra and slated sometime late this year or early next, will include "the first step" to improving EVMs – a series of proposals specifying a new version of EVM code, Buterin said.

The code – called EVM Object Format (EOF) – would, among many other features, separate code and data, which aims to make it easier for layer 2 blockchains to process code.

"Arguably, a roadmap which prioritizes continued improvement to the Ethereum L1 would include and build on EOF," Buterin wrote.

Another proposal slated for launch in Pectra would make account abstraction's "convenience features" available to all users, Buterin said. Account abstraction means users could use a wallet-like smart contract, greatly increasing the range of ways they could interact with the blockchain.

One convenience feature Buterin noted was the ability for an account to pay transaction fees with ERC-20 tokens; now, users can only pay in Ether.

"The main remaining thing to figure out is how to fully bring account abstraction into the protocol," he said. "A recently popular enshrined account abstraction EIP is EIP-7701, which implements account abstraction on top of EOF."

Separately, Buterin discussed Ethereum's transaction fee economics, where he pitched "multidimensional gas," which he described as "having separate prices and limits for separate resources" in order to better price the blockchain's available resources.

"We have multidimensional gas for execution and blobs today," he explained. "In principle, we could increase this to more dimensions: call data, state reads/writes, and state size expansion."

He claimed multidimensional gas could reduce "worst-case" uses of resources, which would "reduce pressure on the need to optimize performance."

7. Post-Quantum Cryptography Market Forecast 2031|ID Quantique, SeQureNet, Quintessence Labs, MagiQ Technologies

https://www.openpr.com/news/3710945/post-quantum-cryptography-market-forecast-2031-id-quantique

Post-Quantum Cryptography (PQC) is revolutionizing the way we think about data security in an age marked by rapid technological advancements and growing cyber threats. At its core, PQC refers to cryptographic algorithms designed to protect data against the potential threats posed by quantum computing. Quantum computers, by leveraging the principles of quantum mechanics, can efficiently solve problems that are currently considered intractable for classical computers. This capability raises significant concerns for traditional encryption methods, which could be easily compromised by future quantum-enabled attacks. Therefore, PQC is not merely an evolutionary step in data protection; it is a critical intervention that ensures the security of sensitive information across multiple sectors, including finance, healthcare, and government operations. The timeliness of adopting PQC solutions has never been more pronounced, as organizations strive to enhance their cybersecurity frameworks amidst escalating threats and to remain compliant with global data protection regulations.

The Post-Quantum Cryptography market is poised for robust growth as both established and emerging players recognize the imminent need for quantum-resistant solutions. Over the next few years, the demand for PQC technologies will continue to soar, driven by high-profile cyber incidents and the looming capabilities of quantum technology. Organizations already operating in the encryption and cybersecurity domains stand to gain substantial advantages by integrating PQC into their services, as they can provide enhanced protection and build greater trust with their customers. For new entrants, this market is brimming with potential, offering opportunities for innovation and market differentiation. With national and global initiatives pushing for the adoption of PQC standards, such as the National Institute of Standards and Technology's (NIST) post-quantum cryptography standardization project, investors are encouraged to explore the myriad possibilities in creating or expanding their PQC offerings.

Reflecting on the evolution of the Post-Quantum Cryptography market reveals a landscape marked by increasing urgency and innovation. Initially, security professionals and technologists were hesitant about the reality of quantum computing threats, often considering the transition to PQC as a long-term requirement. However, recent developments in quantum computing capabilities have accelerated the transition. Today, a range of PQC solutions is gaining traction, with several major players already actively developing and

deploying quantum-resistant algorithms, demonstrating considerable competitive advantages in securing contracts and stakeholder trust. While some challenges like talent shortages, legislative hurdles, and technological gaps remain, they also present opportunities for companies that are ready to adapt and invest in PQC capabilities. As organizations increasingly recognize the importance of preemptive measures against quantum threats, the market outlook.

The latest report by A2z Market Research offers a comprehensive analysis of the Global Post-Quantum Cryptography Market, delivering in-depth insights into current trends, growth drivers, and market dynamics. Tailored for industry stakeholders, this report highlights the essential factors driving the growth of the Post-Quantum Cryptography market, as well as emerging opportunities across multiple industries.

The report also includes advanced customization options, ensuring a detailed understanding of key market segments, including product-level pricing, production capacities, and regional sales volumes. Whether companies are focused on global or region-specific data, this report provides the necessary segmentation to refine strategies and uncover new business avenues.

The Post-Quantum Cryptography market is witnessing a significant shift as technological innovations and enhanced distribution strategies reshape industry landscapes. Businesses can capitalize on these developments to achieve market leadership by gaining a competitive edge in the expanding Post-Quantum Cryptography market.

The competitive landscape of the Post-Quantum Cryptography market is marked by several key players and a high degree of competition among Tier 1, Tier 2, and Tier 3 companies. Major companies such as

Major companies profiled in this report are

- ID Quantique
- SeQureNet
- Quintessence Labs
- MagiQ Technologies
- Toshiba
- QuantumCTek
- Qasky
- Qudoor

leading the market through strategic investments in research and development, mergers and acquisitions, and enhanced production capacities. With the rise of startups and second-tier players, the market concentration ratio is shifting, offering new opportunities for businesses at all levels. The report provides an analysis of company-specific distributors, production capacities, and market share, along with insights into manufacturing processes. It also highlights the role of new entrants in disrupting the market by introducing innovative products or business models. In-depth analysis of company market share at the global, regional, and country levels offers insights into strategic movements in the competitive landscape. Additional

competitors' analysis is available on request, allowing for an even more customized overview of market dynamics.

Several transformative trends are shaping the future of the Post-Quantum Cryptography market The report also offers a deep dive into industry benchmarks, technology development analyses, and winning strategies, enabling businesses to anticipate future shifts in market trends. Heat map analysis and strategic benchmarking provide an edge for companies to optimize their positioning in this evolving market.

The future of the Post-Quantum Cryptography market looks promising, with significant growth opportunities in both established and emerging markets. The report offers customized insights into key regions such as the Americas, Asia-Pacific, and Europe, providing data on production capacities, pricing trends, and market shares at both the regional and country levels.

The Post-Quantum Cryptography market is segmented on the basis of

Type: Lattice-based Cryptography, Multivariate Cryptography, Hash-based Cryptography, Code-based Cryptography

Application: Financial, Government, Military & Defense, Others

The report meticulously segments the Post-Quantum Cryptography market by product type, application, region, and other factors, allowing businesses to understand the demand and supply dynamics at a deeper level. Segmentation customization options include additional countries, cross-split segments, and production analysis for different tiers.

Furthermore, companies can request additional segmentation at the regional, country, and even company levels, enabling them to analyze specific markets and customize their strategies to align with regional demands. Customization at the regional level offers insights into production volumes and sales data in specific combinations like Nordics or DACH, giving businesses a clearer understanding of local market conditions.

The report's in-depth value chain analysis, price trend analysis, and customer sentiment analysis provide a strategic framework for companies to navigate these risks and seize new opportunities. Furthermore, market entry and exit consulting is available for businesses looking to explore new avenues or restructure their operations.

For businesses and investors looking to gain a competitive advantage in the rapidly growing Post-Quantum Cryptography market, the full report offers comprehensive insights into key trends, competitive dynamics, and growth opportunities. Whether you need a global overview or specific regional data customization, this report provides the detailed analysis necessary to make informed decisions.

8. Round 2 PQC Additional Signatures: Multivariate and MPC-in-the-Head To The Fore

by Prof Bill Buchanan OBE FRSE
https://billatnapier.medium.com/round-2-pqc-additional-signatures-multivariate-and-mpc-in-the-head-to-the-fore-007188bfff10

And, so, Dilithium, FALCON and SPHINCS+ have become NIST standards for digital signatures, and with an aim to remove RSA, ECDSA and EdDSA. But, NIST wants alternatives to these, especially so that we are not too dependent on lattice-based approaches (such as with Dilithium and FALCON). In Round 1, these were here:

- **Multivariate Signatures (10):** 3WISE, DME-Sign, HPPC (Hidden Product of Polynomial Composition), **MAYO**, PROV (PRovable unbalanced Oil and Vinegar), **QR-UOV**, **SNOVA**, TUOV (Triangular Unbalanced Oil and Vinegar), **UOV** (Unbalanced Oil and Vinegar), and VOX.

- **MPC-in-the-Head Signatures (7):** Biscuit, **MIRA**, MiRitH (MinRank in the Head), **MQOM** (MQ on my Mind), **PERK**, **RYDE**, and **SDitH** (Syndrome Decoding in the Head).

- **Lattice-based Signatures (6):** EagleSign, EHTv3 and EHTv4, HAETAE, **HAWK**, HuFu (Hash-and-Sign Signatures From Powerful Gadgets), and SQUIRRELS (Square Unstructured Integer Euclidean Lattice Signature).

- **Code-based Signatures (5): CROSS** (Codes and Restricted Objects Signature), Enhanced pqsigRM, FuLeeca, **LESS** (Linear Equivalence), MEDS (Matrix Equivalence Digital Signature).

- **Symmetric-based Signatures (4):** AIMer, Ascon-Sign, **FAEST**, and SPHINCS-alpha.

- **Other Signatures (4):** ALTEQ, eMLE-Sig 2.0 (Embedded Multilayer Equations with Heavy Layer Randomization), KAZ-SIGN (Kriptografi Atasi Zarah), Preon, and Xifrat1-Sign.

- **Isogeny Signatures (1): SQIsign**.

Now NIST has announced Round 2 Additional Digital Signature Candidates [here]:

- **Multivariate Signatures (4): MAYO**, **QR-UOV**, **SNOVA**, **and UOV**(Unbalanced Oil and Vinegar).

- **MPC-in-the-Head Signatures (5): MIRA/MiRitH** (MinRank in the Head), **MQOM** (MQ on my Mind), **PERK**, **RYDE**, and **SDitH** (Syndrome Decoding in the Head).

- **Lattice-based Signatures (1): HAWK.**
- **Code-based Signatures (2): CROSS** (Codes and Restricted Objects Signature), and **LESS** (Linear Equivalence)

- **Symmetric-based Signatures (1): FAEST.**

- **Isogeny Signatures (1): SQIsign**.

We can see that multivariate and MPC-in-the-head signatures are by far the most popular. It is surprising that Raccon has not been selected. It has some excellent features and is perhaps better than Dilithium. But I suppose being a lattice method counted against it (as NIST want an alternative to lattice methods):

Overall, here are some of the methods that have made it to Round 2:

- **CROSS**. CROSS. CROSS (Codes and Restricted Objects Signature) method. With this we use a Fiat-Shamir transfer within an interactive Zero Knowledge (ZK) Identification protocol. Overall it uses the Restricted Syndrome Decoding Problem (R-SDP) as its base, and which was first introduced in "A new path to code-based signatures via identification schemes with restricted errors".

- **FAEST**. FAEST. NIST approved Dilithium, Falcon and SPHINCS+ for PQC digital signatures and is now looking at other alternative signatures. One of these is the FAEST digital signature algorithm [1], and which uses symmetric key primitives. This links directly to the security of AES128 (Level 1), AES192 (Level 3) and AES256 (Level 5). A key pair (pk,sk) is defined as: $pk=(x,y)$ and $sk=k$ and where $Ek(x)=y$. Overall, E is the block cipher to use, k is the private key, and x is a plaintext block. The signature then becomes a non-interactive argument of knowledge of sk. This is similar to the Picnic method, but rather than using the MPC-in-the-Head (MPCitH) framework, it uses the VOLE-in-the-Head method [2].

- **LESS**. LESS. LESS (Linear Equivalence Signature Scheme) is a code-based Post Quantum Cryptography method. It uses Fiat-Shamir transformation onto a zero-knowledge identification scheme. It uses a one-round Sigma protocol. The security of LESS depends on the hardness of the Linear Equivalence Problem (LEP). It has a fairly large public key (13,940 bytes for Level 1), and a small private key (32 bytes for Level 1). The signature size is 9,286 bytes (for Level 1). It is relatively slow for signing and verification.

- **HAWK**. HAWK. HAWK is a lattice-based signature method that creates signatures using the lattice isomorphism problem (LIP) [1,2]. It is faster than Dilithium for signing and verification. It also has a low memory footprint and is supported on a range of hardware. There is currently no masking function, which could be suspectable to side-channel analysis. There are some worries about the security proofs involved with HAWK.

- **MiRitH**. MiRitH. MiRitH (MinRank in the Head) is a quantum robust digital signature method for MPC-in-the-Head Signatures. It is based on the hardness of the MinRank problem. This is a problem that must find a non-trivial low-rank linear combination of defined matrices over a finite field. Mirith uses a MPC-in-the-Head (MPCitH) based Zero-Knowledge Proof of Knowledge (ZKPoK) that relates to a solution of the MinRank problem, and then is converted to a non-interactive signature scheme using the Fiat–Shamir transform. For Level I-a, it has a relatively small public and private key of 129 and 145 bytes, and a reasonable size of signature of 7,877 bytes.

- **PERK**. PERK. PERK is a quantum robust digital signature method that uses a zero-knowledge proof based on a variant of the Permuted Kernel Problem (PKP) and with hash functions as random oracles. This is an MPC-in-the-head approach, and which is then converted into a Fiat-Shamir transform. PERK has a relatively small public and private key, and moderate signature sizes. It also uses symmetric key methods, and thus has good performance levels.

- **Ryde**. Ryde. The Ryde signature method [1] uses the Rank Syndrome Decoding problem as a hard problem. With this, we can create a proof of knowledge of a witness to a Rank-SD instance [2], and then transform this with a Fiat-Shamir transform. It produces relatively short keys but a larger signature compared with Dilithium.

- **SQISign**. Here.

Current standards

The current standards are:

Falcon. Falcon. Falcon is a NIST-approved standard PQC (Post Quantum Cryptography) digital signature. It is derived from NTRU ((Nth degree-truncated polynomial ring units) and is a lattice-based methods for quantum robust digital signing. Falcon is based on the Gentry, Peikert and Vaikuntanathan method for generating lattice-based signature schemes, along with a trapdoor sampler -– Fast Fourier sampling. We select three parameters: N, p and q. To generate the key pair, we select two polynomials: f and g. From these we compute: F=fq=f−1(modq) and where f and fq are the private keys. The public key is h=p·fq.f(modq). With Falcon-512 (which has an equivalent security to RSA-2048), we generate a public key of 897 bytes, and a signature size of 666 bytes, while FALCON-1024 gives a public key of 1,793 bytes and a signature size of 1,280 bytes.

Dilithium. Dilithium. At present, CRYSTALS (Cryptographic Suite for Algebraic Lattices) supports two quantum robust mechanisms: Kyber for key-encapsulation mechanism (KEM) and key exchange; and Dilithium for a digital signature algorithm. CRYSTALS Dilithium uses lattice-based Fiat-Shamir schemes, and produces one of the smallest signatures of all the post-quantum methods, and with relatively small public and private key sizes. The three main implements for the parameters used are: Dilithium 2, Dilithium 3 and Dilithium 5. Overall, Dilithium 3 is equivalent to a 128-bit signature and is perhaps the starting point for an implementation.

9. Can this cryptography tool secure your supply chain data?

https://www.siliconrepublic.com/enterprise/cryptography-tool-secure-supply-chain-data-fully-homomorphic-encryption

Zama's Prof Nigel Smart spoke to Prof Florian Kerschbaum about the challenges of harnessing data to make supply chains more efficient while protecting privacy.

When most people think of supply chains, they rarely associate them with data sets and advanced technology: such a term is more likely to conjure up images of steel containers, cargo ships and warehouses packed to the ceiling with goods.

However, in the digital era, these elements play a crucial role in the modern supply chain management, which has become so much more than simple logistics and moving products.

Now more than ever, managing the end-to-end flow of goods is a complex matter that involves a number of actors and functions, from infrastructures to human resources; people have to constantly communicate, sharing information about the items from production to final delivery.

The same way large data sets are proving important with cutting-edge technologies such as AI and machine learning, they are also impacting the complex network of entities involved in the supply chain.

In this context, the quality and quantity of information available becomes crucial to ensure efficient completion of the supply chain cycle, which contributes significantly to the production costs and, ultimately, the price for consumers.

The value of data

According to Prof Florian Kerschbaum, the increasing weight of data has the potential to overcome some of the most common setbacks in the sector.

"Managing supply chains is one of the most complicated tasks in business management. It requires the collaboration of many parties which often have diverging interests," explained Kerschbaum, who is a professor at the David R Cheriton School of Computer Science, University of Waterloo.

"Supply chains can be a major source of inefficiencies.

"However, often the sources of the inefficiencies are not well known. This is one area where data collection across the supply chain can help: collecting information for the analysis of inefficiencies."

Being able to collect and analyse accurate data can help with aspects that have become increasingly important in recent years, not just for the companies producing and trading goods but also for the end consumers.

Kerschbaum identifies three key areas: traceability is now a basic requirement for most foods, produce and beverages, potentially preventing risk of contamination as well as counterfeiting; most companies have developed a keen interest for sustainability, something that has become a selling point and seal of commitment beyond business for many organisations; finally, compliance is another key factor, essential from start to finish to avoid failures throughout the process.

"Tracking of sustainability goals across the supply chain requires parties to share data. Ethical sourcing of materials is becoming a major differentiator.

"Compliance, for example, in the medical supply chain, similarly requires tracing each product throughout its entire life cycle," Kerschbaum notes.

"Much data needs to be exchanged between the parties and delivered in a reliable manner to the customer. In the case of compliance, such data exchange must fulfil a legal objective, but what and how data is shared can vary on the technical implementation."

Data collection is obviously not new for supply chain management; however, this was previously limited by the equipment required and the technology available.

Kerschbaum highlights the main difficulties in updating the practice as cost to replace the equipment and the relative delay on amortising the investment.

"However," he notes, "due to the lower costs of scanning equipment, essentially mobile phones, and the success of barcodes, many manufacturing and transportation facilities are now better equipped to collect this valuable data along the supply chain."

Protecting your data

Where there is data, there is inevitably the risk of exposing information you'd rather keep private.

This might be a familiar concern for private citizens, used as they are to the daily trade-off of sharing personal information to access services, entertainment platforms and to buy products.

As seen so far, in the supply-chain-management world data has a very specific weight and requires matching levels of infrastructure and skills to be collected, stored and managed efficiently. But efficiency is only one side of the coin; one aspect that should be driving any activity related to the big volume of sensitive data is privacy.

Privacy is not just about data ownership or security; it's about being able to selectively disclose what you want to whom you want, especially when not given a choice.

Since the introduction of regulations such as GDPR, users have been given more power over what happens with their personal information; they can limit the collection, have a say in the way information is stored and for what purpose they can be used and even request for data to be deleted.

However, as the power of data increases and is applied to more and more industries and sectors, it becomes vital to raise awareness on the privacy risks related to this particular resource. Thus, the controls you now expect for personal data, are becoming increasingly important for corporate data as well.

Kerschbaum says the confidentiality of the information in the supply chain can be cut in many different ways.

"While the economic benefits of supply chain data are obvious to the outside expert, sharing this data can come with many risks to the parties involved. As mentioned at the outset, the parties may have diverging interests, often maximising their own profit.

"What if this data reveals that one's company is the major source of inefficiency? Will one be able to ask for the same price in a future negotiation? Will one even be invited to the next negotiation?

"Even data that is collected for the purposes of compliance or sustainability goals may inadvertently reveal inefficiencies if shared in plain. The finer-grained the data, the more analyses it enables, for the good and for observing your supplier."

Finding the right key

These dilemmas naturally lead to a simple yet rather direct question: how can the supply chain sector as a whole enjoy the assets provided by data without compromising the privacy and resources of the individual actors involved?

An efficient solution already exists, provided by cryptography. This might seem an odd pairing, but cryptography is at the core of most of the technologies commonly applied to protect data privacy.

And while there are many options available for developers to choose from – multi-party computation, zero knowledge proof, data anonymisation and federated learning to name a few – most of them present a downside that limits their widespread adoption, whether because of the speed, the risk of data leaks or the use of external servers.

There is however an encryption technique capable of providing the desired balance between the privacy of data and the need to elaborate these without putting that at risk.

What is fully homomorphic encryption?

Fully homomorphic encryption (FHE) enables data to be processed blindly without having to decrypt it; this means that different actors can execute operations on a set of data without accessing the complete set.

In supply chain management, the use of FHE-based tools would allow companies to encrypt and securely share data about the movement and authenticity of goods. Businesses can collaborate and share information to track goods from production to delivery without revealing proprietary information or business secrets; this is particularly valuable in combating counterfeit products and ensuring the integrity of the supply chain, enhancing transparency and trust among supply chain partners while protecting competitive advantages.

This also enables more economically and environmentally efficient supply chains.

Imagine a container ship owner who wants to sell their spare capacity, and a manufacturer or supplier of goods who wants to purchase this capacity; if the precise supply was known to be very large, then the purchaser may try to enforce a lower price, but on the flip side, if the precise demand was known to be large, then the supplier may try to enforce a higher price.

This allocation of resources problem is much like an auction. We wish to allocate the resource (the shipping capacity) between the supplier and the purchaser at a fair price. We also want all the capacity to be used, to reduce greenhouse gas emissions, for example. A technology such as FHE enables private auctions to be carried out; as we have seen, such auctions are not only important in areas where one traditionally associates auctions (e.g., in finance), but also in areas such as supply chain management.

Another application could be to keep only certain data private in a siloed approach, for example by selectively revealing only certain parts of the information related to a shipment to the necessary people. Not all parties in the entire supply chain for an item need to know the final destination or original source of an item, or even the specific hops which a shipment has made.

By using FHE, we can process data securely, and selectively reveal sensitive data to parties as and when required.

10. Quantum computer ‘threat’ to crypto is exaggerated — for now

by ANDREW SINGER
https://cointelegraph.com/news/quantum-computing-bitcoin-encryption-keys

A report that Chinese researchers have employed a D-Wave quantum computer to breach encryption algorithms used to secure bank accounts, top-secret military data and crypto wallets is, at first glance, a matter of deep concern.

"This is the first time that a real quantum computer has posed a real and substantial threat to multiple full-scale SPN [substitution-permutation network] structured algorithms in use today," wrote Shanghai University scientists in a peer-reviewed paper, according to an Oct. 11 report in the South China Morning Post (SCMP).

The paper talks about breaking RSA (Rivest-Shamir-Adleman) encryption, one of the oldest and most widely used public-key cryptosystems.

Details about the latest research have been slow to emerge, so it's difficult to say for sure how dire the threat is to cryptocurrencies and blockchain technology. The paper had yet to be released in English as of Oct. 11, and researchers weren't taking any interviews, supposedly "due to the sensitivity of the topic," according to SCMP.

But if the researchers' results hold up and can be duplicated by others, "it is a step forward" in the evolution of quantum computing, Marek Narozniak, a physicist with a background in quantum computing and the founder of Sqrtxx.com, told Cointelegraph.

Would it mean that the password-protection mechanisms used in many industries, including banking and cryptocurrencies, might soon be vulnerable, as many fear?

"From the paper, many details are missing, so it is difficult to provide a definite answer" with regard to its possible significance, Massimiliano Sala, a full professor and the head of the Laboratory of Cryptography at the University of Trento, told Cointelegraph.

Much depends on whether the scientists were able to break RSA keys of a certain size — i.e., keys as large as those used by banks to secure customers' savings and checking accounts today. "There is no evidence of that," said Sala.

But if they had, it would be "huge," he said.

Quantum computing (QC), which uses atomic "spin" instead of an electrical charge to represent its binary 1s and 0s, is evolving at an exponential rate, many say. But full purpose QC devices have yet to emerge at scale.

The D-Wave machines used in Shanghai, sometimes called quantum annealers, are really proto-quantum computers, or forerunners, capable of conducting specialized tasks only.

However, if and when universal quantum computers do emerge, some worry they could threaten the elliptic curve cryptographic structure that has served Bitcoin and other cryptocurrencies very well until now.

It could only be a matter of time before quantum computers are able to identify the enormous prime numbers that are key constituents of a Bitcoin private key – assuming no countermeasures are developed.

"We must keep in mind that D-Wave quantum computers are not general-purpose quantum computers," added Sala. Moreover, D-Wave's "ability to factor RSA keys was already established by one of my colleagues a few months ago," he said.

Takaya Miyano, a professor of mechanical engineering at Japan's Ritsumeikan University, also questioned the significance of the scientists' results – and along similar lines as Sala.

The length of the integer that the Shanghai researchers factorized, 22 bits, "is much shorter than that of actual RSA integers, which is usually equal to or greater than 1,024 bits – e.g., 1,024, 2,048, and maximally, 4,096 bits," he told Cointelegraph.

Moreover, "the D-wave machine is a kind of quantum simulator for solving optimization problems, not a universal computer," Miyano added. It isn't clear that it would be able to conduct rapid factorization of large RSA integers in the real world.

Why prime factorization is important

Factorization is a mathematical process where a number can be written as the product of smaller whole numbers. For instance, 12 can be factorized, or written, as 3 x 2 x 2. Efficient prime number factorization has been called "the holy grail" of breaking an RSA public-key cryptosystem.

RSA is more than encryption, after all. It is also a "key" generation scheme that typically involves multiplying large prime numbers. Two parties – a bank and its customer, for example – typically receive a set of prime numbers that are used to compute their private and public keys, Narozniak explained.

The process of actually generating private and public keys is complex, but if "p" and "q" are prime numbers, and "n" is the product of those two prime numbers (i.e., n = p x q), then one can say that p and q are related to the private keys and n is related to the public key.

The basic mathematical principle behind RSA encryption is that while it is easy to multiply two prime numbers, it is very difficult to do the reverse – i.e., find the two prime numbers that are factors of a product – and this becomes harder as the numbers get larger.

Sala's University of Trento colleagues earlier this year used a quantum annealer to uncover the two prime factors of the number 8,219,999 (32,749 and 251), "which, to the best of our knowledge, is the largest number which was ever factorized by means of a quantum device," wrote the researchers.

In Sala's view, the recent Shanghai University paper is significant "only if they have found a way to factorize huge numbers."

The University of Trento researchers also cited the great potential of quantum computing to solve complex problems that have long remained "intractable" for classical computers.

Prime factorization – the problem of breaking down a number into its prime factors – in particular, "is a good candidate to be effectively solved by quantum computing, in particular by quantum annealing."

Crypto keys are safe – for now

Let's assume, however, that the Shanghai scientists really did find a way to use a quantum annealer to successfully breach cryptographic algorithms, including those like SPN, which are foundational for the advanced encryption standard (AES) widely used in the military and finance. What would that do to the crypto industry?

"Symmetric ciphers such as AES-128 used for data encryption are not vulnerable to this kind of attack, as they do not rely on number factorization," said Narozniak.

There might be exceptions, of course, like if the cipher is a shared secret derived via RSA-based key exchange protocol, he continued. But "properly encrypted passwords and other data in general will remain encrypted even if the approach presented in that research scales up and becomes widely available – and if true," he said.

A history of unproven RSA claims

Narozniak cautioned against rushing to conclusions. "Before we reevaluate our level of optimism, let us wait for someone to repeat and confirm this result," he said. "Claims of breaking RSA are not so uncommon."

In early 2023, for instance, Chinese researchers said they had factorized a 48-bit key on a 10-qubit quantum computer, a claim "which still has not been peer-reviewed," commented Narozniak. "And two years before that, Claus Schnorr, who is an authority in the community, made an honest mistake and claimed RSA to be broken. I personally take such big claims with a grain of salt."

According to Sala: "Breaking RSA would mean that a lot of software should be updated, but not drastically changed," because there are already-implemented standards that provide alternatives, including elliptic curve cryptography (ECC), used to secure Bitcoin. He added:

"More drastic would be the impact on credit cards and the like, which would have to be withdrawn massively, to radically change their software."

One might wonder why cryptocurrencies don't use RSA widely, as banks do. The crypto industry favors elliptic-curve cryptography because it makes it possible to achieve the same level of security with much smaller keys using fewer bytes, said Narozniak. This opens up digital space, which enables chains to grow faster.

Is Buterin's "hard fork" solution viable?

Elsewhere, Ethereum co-founder Vitalik Buterin suggested in March that a "hard fork" could subvert a quantum attack on Ethereum were it to arise. "We are already well-positioned to make a pretty simple recovery fork to deal with such a situation," he posted on Oct. 17. Users might have to download new wallet software, but few would lose funds.

Is it really so easy, though? "I disagree that such a hard fork would be 'simple,'" said Narozniak. And looking ahead, quantum-safe signatures, such as ML-DSA, would need to have significantly larger keys and signatures compared with those used today. This could slow onchain performance and raise gas fees, he suggested.

Executing a hard fork would "be complex, require broad community consensus, and may not restore all lost assets or fully repair trust in the network," Samuel Mugel, chief technology officer at Multiverse Computing, told Cointelegraph. "Therefore, it's crucial to implement quantum-resistant cryptography before such an attack happens to avoid this situation."

Safeguards are needed

"We most certainly need to revisit our current cybersecurity defenses," Christos Makridis, associate research professor at Arizona State University and founder and CEO of Dainamic, told Cointelegraph.

More attention needs to be paid to network capacity loads (i.e., defending against distributed denial of service attacks) and to passwords (e.g., to protect data from hackers) in a world with quantum computing. He further observed:

"One of the emerging views is that the expansion of quantum computing and generative AI has enabled offensive cyber more than defensive."

The industry can't become complacent. "Dangerous quantum computers will come, it's just a matter of time," Sala warned.

"The blockchain world must get ready as soon as possible, by planning a roadmap towards a transition to post-quantum cryptography," he added, developing safeguards able to resist attack even by a "fully-fledged quantum adversary."

11. Why IT Leaders are Fast-Tracking Post-Quantum Cryptography

by Kitty Wheeler
https://technologymagazine.com/articles/why-it-leaders-are-fast-tracking-post-quantum-cryptography

Global technology is on the cusp of a significant shift as quantum computing advances threaten to undermine current encryption methods.

This impending change has far-reaching implications for data security across industries and governments worldwide.

Quantum computers, which leverage the principles of quantum mechanics to perform complex calculations, have the potential to break many of the cryptographic systems currently used to protect sensitive information.

In response to this looming threat, organisations and government agencies are increasingly turning their attention to post-quantum cryptography (PQC), which refers to cryptographic algorithms designed to be secure against both quantum and classical computers.

As the race to develop quantum computers intensifies, the need for robust PQC solutions becomes more pressing, particularly for entities handling sensitive data and critical infrastructure.

In light of this race, a recent study by General Dynamics Information Technology (GDIT), a technology services provider for government and commercial customers, reveals that 50% of federal IT leaders in the US are actively developing strategies to accelerate their transition to post-quantum cryptography.

US federal agencies prioritise PQC readiness

The research, titled "Quantum Waves", surveyed 200 experts and decision-makers across defence, civilian and intelligence agencies.

It aimed to explore how these agencies are addressing the PQC transition and identifying risks, challenges and technologies needed for migration.

According to the research, 35% of respondents are in the process of defining their plans and budgets for PQC readiness.

This indicates a growing awareness of the urgency to prepare for a post-quantum future.

Ben Gianni, Senior Vice President and Chief Technology Officer at GDIT says:

"*With finalised NIST PQC standards, agencies must accelerate their migration efforts. By developing flexible and scalable strategies today, they will be prepared to modernise and build long-term resilience against emerging quantum threats.*"

The study also found that 46% of respondents have identified key risks associated with current cryptographic practices but have not yet begun formal assessments.

Only 8% have fully integrated current PQC standards, highlighting the nascent stage of PQC adoption in many federal agencies.

Challenges in PQC adoption

Yet despite the momentum in PQC planning, the research uncovered significant obstacles facing federal agencies in their transition efforts.

KEY STATS FROM THE SURVEY REGARDING BUILDING PQC MOMENTUM

- 50% are developing strategies for PQC readiness
- 22% are engaged in pilot projects
- 12% are preparing the workforce
- 17% has yet to prioritise PQC initiatives

GDIT reports that 37% of respondents cited the lack of formal guidance and strategic frameworks as a major challenge.

This suggests a need for clearer directives and standardised approaches to guide agencies through the complex process of PQC adoption.

Modernising legacy systems also remains a significant hurdle, with 48% of respondents identifying this as a key challenge.

The implications for operational technology, which encompasses the interconnected systems controlling physical operations in critical infrastructure, were cited as a concern by 29% of respondents.

Additionally, 24% of those surveyed reported difficulties in integrating PQC into their supply chains, indicating the far-reaching implications of this technological shift.

GDIT highlights the importance of vulnerability management in facilitating the transition to PQC.

According to the report, 44% of respondents identified vulnerability management as a top capability needed to discover, assess and manage cryptographic assets, prioritise risks and accelerate the PQC transition.

Ben emphasises the critical nature of this transition: "Quantum computing represents a turning point for cybersecurity, and achieving cryptographic agility is critical to secure our sensitive information against future threats."

12. Are WhatsApp and Signal Secure Enough for Confidential or Secret Communications?

by David Wiseman
https://blogs.blackberry.com/en/2024/10/whatsapp-signal-secure-enough-corporate-government-messaging

Are consumer level encrypted communication tools like WhatsApp and Signal secure enough for your organization's confidential data? And how about secret military or government communications? I'm repeatedly asked these questions. The answer is, it depends both on what you need and what you expect.

In my role, I work with militaries, all seven of the G7 governments, eight of the ten largest banks and half the Fortune 100. These organizations have something in common: they've realized that limiting espionage and sensitive data loss due to intercepted communications is a key element of holistic cyber defense. As a result we are engaged in constant discussions about BlackBerry® SecuSUITE® our secure communication platform.

The Difference Between Consumer Encryption Apps and BlackBerry

What is the difference between consumer grade apps and something like SecuSUITE? Well, I recently appeared on a Land Forces 2024 podcast, where host Grant McHerron asked me about this. Keep reading for a portion of our dialogue or listen to the complete interview for yourself.

My response: Well, when we look at Signal and look at WhatsApp, they both use the same cryptography. And there is nothing wrong with that cryptography! However, cryptography is just a small portion of the secure communication challenges you need to address.

Additionally, when you talk about the most sensitive communications for militaries, for executives, for foreign affairs and parts of the government – they need to have something where they have control over the system.

Control means several things. For one thing, it means understanding where the data resides, they need to know they have control over the computing architecture or environment of that system. And even more importantly, they have control over the users.

In this case, by control, I also mean they're specifically authorizing people to be part of that secure communication network, whereas with a Signal or WhatsApp, you self-register. This leads to a lot of the issues around identity spoofing, identity fraud and worrying about deep fakes. Anytime you have an open system where people self-register that is very high risk.

And then another part that comes into that is, it's one thing – and it's important – to encrypt the conversation strongly, whether you and I would talk over the phone or through messages. But there's also all the associated metadata information, who's calling whom, who's messaging whom and for how long?

I'm sure you've seen the police movies where they start drawing the strings on the board with all the connections? That's exactly what metadata is. Recognizing the value of that from an intelligence perspective, we actually encrypt that data as well and put it into a tunnel so that it's not visible to anyone else but the actual customer. Therefore, an adversary cannot capture and harvest the metadata.

Podcast Host: *Let's say I'm, for instance, a large corporation. I want to make sure I'm securing the comms between my executives. How do we go about getting that set up? How does BlackBerry go about making sure that my data is in my country, not on a server somewhere in North America, or the world or things like that? I mean, you're Canadian, so we like you and all that kind of stuff, but how do we ensure this?*

My Response: We provide two approaches, let's begin with the first one. Normally, if it's a commercial organization, we're going to provide software as a service (Saas), a cloud-based system. And one of the key things about the data is we don't store the customer's data in our system. It's just there on a temporary basis while the message is delivered and then it's gone.

At the government level, and for some of the organizations like those in critical infrastructure, some of those highly regulated organizations, we actually provide the ability for them to deploy the back-end system in their own cloud and their own data center, and so there's no connectivity to any BlackBerry networks or storage or anything at all in that sense. We have a discussion with each customer asking about their risk level and regulatory requirements, and then based on that we'll help them with the right deployment method.

The second approach we take is to focus on the actual people using the system. If they write a message or they send a document, then they own and control that document. They control the lifecycle, so even if it's a year down the road, they can pull that document back or they can pull a photo back.

And that's a fundamentally different model than you get with a consumer system like Signal or WhatsApp. The model there for consumer apps is, you might be able to temporarily edit or change something for a few minutes or a few hours, but once you give somebody data, it's their data. Our BlackBerry SecuSUITE model

is different. What's sent is the company's data or the government's data – and the person that's making the decision to send it – can control it and pull that back.

13. WeChat devs introduced security flaws when they modded TLS, say researchers

by Connor Jones
https://www.theregister.com/2024/10/17/wechat_devs_modded_tls_introducing/

Messaging giant WeChat uses a network protocol that the app's developers modified – and by doing so introduced security weaknesses, researchers claim.

WeChat uses MMTLS, a cryptographic protocol heavily based on TLS 1.3. The devs essentially tweaked standard TLS but in turn that left the app with an encryption implementation, which "is inconsistent with the level of cryptography you would expect in an app used by a billion users, such as its use of deterministic IVs and lack of forward secrecy."That's according to the University of Toronto's Citizen Lab, which carried out a comprehensive review of MMTLS's network security.

It identified MMTLS in previous work, but a more thorough analysis revealed it offers two layers of encryption instead of one as first thought. Plaintext content is wrapped in what's referred to as "business-layer encryption" and the resulting ciphertext is then wrapped in MMTLS encryption, the ciphertext from which would be sent over the WeChat network.

Researchers found that most of the cryptographic security issues were in WeChat's AES-CBC-based business-layer encryption, which until the introduction of MMTLS in 2016 was the sole layer of encryption for network requests.

In fact, the only reason why researchers weren't able to successfully attack WeChat this time around was because this is now enveloped in MMTLS. Before, various types of attacks were possible such as a padding oracle attack, and just last year Citizen Lab claimed it found a different cryptography scheme developed by a Tencent company was still vulnerable to an attack of this type.

The most serious issue the researchers found, however, was that the business-layer encryption doesn't encrypt metadata such as user IDs and request URIs, leaking them in plain text.

"It could be the case, for instance, that after MMTLS is terminated at the front WeChat servers (handles MMTLS decryption), the inner WeChat request that is forwarded to the corresponding internal WeChat server is not re-encrypted, and therefore solely encrypted using business-layer encryption," said Citizen Lab.

"A network eavesdropper, or network tap, placed within WeChat's intranet could then attack the business-layer encryption on these forwarded requests. However, this scenario is purely conjectural. Tencent's response to our disclosure is concerned with issues in business-layer encryption and implies they are slowly migrating from the more problematic AES-CBC to AES-GCM, so Tencent is also concerned with this."

Ultimately, thanks to the wrapping of ciphertext in MMTLS, there are no vulnerabilities in WeChat's encryption protocol that could lead to any known attacks today. However, the issues described as "minor" ones by the researchers aren't present in the standard, unmodified version of TLS.

Messages sent using WeChat, to the researchers' understanding, are safe from eavesdroppers. Although Tencent would still have to comply with any data requests from the CCP given local laws, and WeChat communications aren't end-to-end encrypted – the app's servers decrypt and read every message, Citizen Lab said.

The researchers may have stumbled on other findings if they had access to the version that's actually used in China. However, given the difficulty in accessing Chinese phone numbers due to government requirements linking them to national IDs, they had to use non-Chinese numbers, which makes the app behave differently.

A trend unique to China

Only in China is it common for developers to go against the grain and whip up their own cryptography system, the researchers said, and generally none of these are as effective as the standard TLS 1.3 or QUIC implementations.

Citizen Lab spotted the same practices across various apps in recent years and despite previous concerns over the TLS certificate authority system, the standard implementations are usually the best options from a security perspective. They described it as "a growing, concerning trend unique to the Chinese security landscape."

Similarly, developers are also known in China to implement custom domain lookup systems to mitigate the pervasive actions of shady ISPs. They often engage in DNS hijacking to display ads or redirect web traffic for ad fraud. It's a longstanding, widespread issue that's been challenged by large internet companies, but it remains a problem nonetheless.

Much of WeChat's code, for example, is taken straight from Tencent Mars – an open source infrastructure component that provides apps with common fundamental functionality such as networking and logging.

Mars has a feature called NewDNS – an example of this bespoke domain lookup system present in WeChat.

The researchers believe Mars is highly prevalent in apps outside of WeChat, which the info-seccers said was a problem given that the component doesn't provide any transport encryption. MMTLS is not part of the open-source Mars component, it's bespoke to WeChat.
Combining this with the lack of formal documentation guiding developers on Mars' implementation – many rely on community wisdom on platforms like GitHub – means mistakes are more likely to occur, leading to potentially weaker security.

Citizen Lab said it suggested to Tencent that it adopt the standard TLS or a combination of QUIC and TLS for better app security.

14. Post-Quantum Cryptology: How Secure Memory Can Protect Against Vulnerabilities

by Jun Kawaguchi
https://www.electronicdesign.com/technologies/embedded/quantum-computing/article/55236010/winbond-preparing-for-post-quantum-cryptography-and-future-cyber-threats

A Fortune Business Insights report revealed that quantum computing was valued at $885 million in 2023 and is projected to grow to $12 million by 2032. Quantum computers can do massive computation for things like blockchain and decrypting encryption.

With the potential to transform many industries such as chemical research and drug discovery, manufacturing (reducing the need for prototyping), supply-chain management, and even AI in the future, quantum computing could also become a significant cybersecurity threat.

Why Post-Quantum Cryptography is Crucial for Future Security

Experts predict this could be a major event by 2030, and organizations should start putting plans in place now. Post-quantum cryptography (PQC) is considered a vital replacement for classical cryptographic algorithms that are no longer considered to be safe in lieu of quantum computers.

In response, the U.S. NSA and U.K. NCSC have adopted Leighton-Micali Signature (LMS) as the preferred PQC algorithms for digitally signing and authenticating firmware and software updates. Compliance with the new Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) guidelines for software and firmware signing is expected by 2025, with a complete transition mandated by 2030.

Similarly, the RED (Radio Equipment Directive) is a European regulation that by the year 2025, anything transmitting over a network must have a cybersecurity provision. Likewise, another European regulation for the automotive industry called the UN R155 claims that manufacturers need to have cybersecurity provisions built into products to counter cybersecurity attacks.

For example, any car that's not prepared by July 1, 2024, will not be allowed to ship. Some automakers are foregoing production on certain models because they decided not to implement those security measures.

Security Risk and the Rise of Connected Vehicles

Automakers are at major risk with the rise of connected vehicles, which must meet high security standards to protect drivers' and passengers' safety and privacy. This can pose significant challenges if automakers don't act now. With the industry's long development cycles over five years, a car developed today will be on the road until at least 2040, according to a McKinsey report.

This issue could also wreak havoc across the supply chain. Adversaries could interrupt supply chains, diminishing supply-chain assurance by intercepting the shipment of a device or even within the factory. Secure MCUs have some level of security, but they lack large memory and the ability to expand memory.

Secure Memory with Post-Quantum Cryptography

Embedding secure memory in the device with data that's encrypted is one way to provide better protection against these attacks. On this front, PQC can be implemented in many ways, including integrating in-memory, which meets the emerging regulations requirements and is designed for applications in industrial IoT, networking, servers, and critical infrastructure applications.

Memory-supporting asymmetric key cryptography algorithms and enabling devices can facilitate both secure over-the-air (OTA) with asymmetric PQC signatures and a secure supply chain via LMS-OTS (NIST 800-208). These secure-memory devices provide robust protection for both code and data, making it difficult for hackers to tamper.

Such devices also employ stringent authentication protocols, ensuring only authorized actors and software layers gain access. On top of that, they facilitate remote secure software updates while safeguarding against rollback attacks, ensuring only legitimate updates are made.

In addition to deploying secure memory in devices, companies can take the following steps to plan for post-quantum threat.

- Conduct an audit of their current security scheme to determine if it's vulnerable.
- Review internal data and determine what's valuable to protect.
- Review hardware and software requirements and start developing a plan to implement the security scheme.
- Ensure software updates are done regularly.
- Work with ecosystem partners, such as memory, networking, and software providers, to put safeguards in place before it becomes more prevalent.

While quantum computing still requires enhancements in scaling, as we've observed with the recent acceleration of generative AI, companies should prepare for rapid advances. This emerging technology poses significant security risks that need to be addressed.

15. Tiny Computer, Big Advance: Taiwan Develops Small Quantum Computer Using Single Photon

by Matt Swayne
https://thequantuminsider.com/2024/10/17/tiny-computer-big-advance-taiwan-develops-small-quantum-computer-using-single-photon/

Taiwanese researchers, led by National Tsing Hua University professor Chuu Chih-sung, have developed what is being described as the world's smallest quantum computer, powered by a single photon. According to the Taipei Times and a university statement, it's not just about being small. This device also represents a significant step forward for quantum computing, particularly in addressing some of the field's key challenges, such as energy efficiency and temperature stability.

The research, which was recently published in the journal Physical Review Applied and arXiv, highlights the team's innovative use of photonics to encode information into 32 time bins – or dimensions – of a single photon. Traditional quantum computers often rely on supercooled environments and complex machinery to function, but this photonic system operates at room temperature, reducing the energy requirements typically associated with quantum devices, reported the *Taipei Times*.

Photonics' Path to Practical Quantum Computing

Photons, or light particles, are central to this new development. Unlike traditional quantum systems that often require sub-zero temperatures to prevent interference, photons can maintain stable quantum states at ambient room temperatures – usually 20°C and 25°C, or 68°F to 77°F, making them more practical for real-world applications. The team believes this stability could offer a competitive edge in the eventual commercialization of quantum computing technologies.

According to Chuu, photonic quantum computing has the potential to overcome some of the common issues that plague other quantum computing models, such as information loss and computational errors caused by external factors like vibrations or magnetic fields. The *Taipei Times* reported that these advantages could place photonic quantum computing at the forefront of efforts to build scalable, commercially viable quantum systems.

Quantum computing differs fundamentally from traditional computing in how information is processed. In classical systems, information is encoded in bits, which are binary and can represent either a 0 or a 1. However, the team explained that quantum computing uses qubits, which can exist in a state of superposition, meaning they can probabilistically represent both 0 and 1, along with a range of other states

in between. This enables quantum computers to perform complex calculations much faster than traditional systems.

Overcoming Energy and Cooling Barriers

One of the biggest challenges in quantum computing has been maintaining stable quantum states in operational environments, the team reports.

Quantum systems are highly sensitive to external influences, requiring elaborate cooling systems to function properly. In an interview with the *Taipei Times*, National Tsing Hua University President John Kao reflected on his visit to a U.S. quantum lab last year, noting that the lab's quantum computer relied on a massive cooling system that filled an entire room, keeping the temperature near absolute zero. In contrast, the Taiwanese photonic quantum computer can operate at room temperature, which drastically simplifies its requirements and opens up new possibilities for deployment in everyday environments.

Kao emphasized that this development marks a crucial milestone for Taiwan in the field of quantum technology. The publication of Chuu's research in a reputable journal like *Physical Review Applied* not only brings attention to the technical progress but also highlights Taiwan's growing role in the global quantum computing landscape.

Taiwan's Broader Quantum Ambitions

Taiwan's government has also been actively supporting the country's quantum computing initiatives. As reported by the *Taipei Times*, the National Science and Technology Council has been spearheading efforts to integrate Taiwan into the international quantum technology ecosystem. This year, the council is hosting the Quantum Taiwan event, possibly featuring Nobel laureate Alain Aspect.

The event will explore a range of quantum technologies, from superconducting quantum computers to quantum communications and sensing. National Science and Technology Council Minister Wu Cheng-wen stated that quantum technology holds the potential to revolutionize computational abilities and enhance the security of communications. Wu also said that global collaboration was critical to the development of quantum, indicating that Taiwan is positioning itself as a key player in the international development of quantum technologies.

While Chuu's single-photon quantum computer is still in the research phase, it does show Taiwan's commitment to advancing quantum technologies in ways that are practical and commercially viable.

16. Debunking Hype: China Hasn't Broken Military Encryption With Quantum

by Craig S. Smith

https://www.forbes.com/sites/craigsmith/2024/10/16/department-of-anti-hype-no-china-hasnt-broken-military-encryption-with-quantum-computers/

Recent headlines have proclaimed that Chinese scientists have hacked "military-grade encryption" using quantum computers, sparking concern and speculation about the future of cybersecurity. The claims, largely stemming from a recent South China Morning Post article about a Chinese academic paper published in May, was picked up by many more serious publications.

However, a closer examination reveals that while Chinese researchers have made incremental advances in quantum computing, the news reports are a huge overstatement.

"Factoring a 50-bit number using a hybrid quantum-classical approach is a far cry from breaking 'military-grade encryption'," said Dr. Erik Garcell, Head of Technical Marketing at Classiq, a quantum algorithm design company.

While advancements have indeed been made, the progress represents incremental steps rather than a paradigm-shifting breakthrough that renders current cryptographic systems obsolete.

"This kind of overstatement does more harm than good," Dr. Garcell said. "Misrepresenting current capabilities as 'breaking military-grade encryption' is not just inaccurate—it's potentially damaging to the field's credibility."

Jason Soroko, senior fellow at Sectigo and co-host of the Root Causes podcast, said that there are no alarm bells ringing. "Quantum resistant algorithms that we are currently working with from the recent NIST standardization are also resistant to Quantum Annealing," he said. NIST is the U.S. National Institute of Standards and Technology.

Dr. Garcell said enterprises should follow NIST's guidance as new encryption standards are developed and rolled out.

In fact, the Chinese paper in question, titled Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage, does not mention military-grade encryption, which typically involves algorithms like the Advanced Encryption Standard (AES).

Instead, the paper is about attacking RSA encryption (RSA stands for Rivest-Shamir-Adleman, named after its creators). RSA is a public-key cryptosystem, one of the oldest and most widely used for secure data transmission, underpinning everything from online banking to secure communications. Its security relies on the computational difficulty of factoring large prime numbers—a task that is feasible for small numbers but becomes exponentially harder as the numbers grow larger.

Quantum computing has long been touted as a potential threat to RSA encryption due to algorithms like Shor's algorithm, which, in theory, can factor large numbers exponentially faster than classical algorithms.

However, practical implementation requires a universal quantum computer with a large number of stable qubits—a feat that remains out of reach with current technology.

Quantum annealing is a different approach to quantum computation, optimized for solving combinatorial optimization problems. Companies like D-Wave Systems have developed quantum annealers that use quantum tunneling to find low-energy states of a system, potentially solving certain types of problems more efficiently than classical computers.

Unlike universal quantum computers, quantum annealers are not generally capable of executing algorithms like Shor's. However, researchers have been exploring ways to map problems like integer factorization onto the quantum annealing framework.

Recent reports highlight work by Chinese researchers at a laboratory at Shanghai University's School of Communication and Information Engineering who have used quantum annealing hardware to factor larger integers than previously accomplished using this method. For instance, factoring numbers up to 50 bits using hybrid quantum-classical algorithms represents progress over earlier efforts that were limited to smaller integers.

The researchers employed innovative techniques to optimize the mapping of the factorization problem onto the quantum annealer. By reducing the number of required qubits and improving the efficiency of the algorithms, they demonstrated the potential for quantum annealing to contribute to cryptographic research.

While factoring a 50-bit integer is an impressive technical achievement, it's important to note that RSA encryption commonly uses key sizes of 2048 bits or higher. The difficulty of factoring increases exponentially with the size of the number, meaning that the gap between 50-bit and 2048-bit integers is astronomically large.

Moreover, the methods used involve a hybrid approach that combines quantum annealing with classical computation. This means that the quantum annealer handles part of the problem, but significant processing is still performed by classical algorithms. The advances do not equate to a scalable method for breaking RSA encryption as it is used in practical applications today.

The media often seeks sensational stories, and the prospect of quantum computers cracking encryption algorithms makes for eye-catching headlines. However, these headlines can be misleading when they suggest that RSA encryption is on the verge of collapse due to new quantum breakthroughs.

In reality, the incremental advances by Chinese researchers are valuable contributions to the field of quantum computing and cryptography. They showcase creative problem-solving and push the boundaries of what current quantum annealing hardware can achieve. Nonetheless, they do not represent a fundamental breakthrough that compromises modern cryptographic systems.

Breaking RSA encryption using quantum computers remains a theoretical possibility that drives ongoing research. Universal quantum computers capable of running Shor's algorithm on practical key sizes would

pose a significant threat to current encryption methods. However, such machines would require thousands or even millions of qubits with low error rates—a technological milestone that is still years, if not decades, away.

In the meantime, researchers continue to explore quantum-resistant cryptographic algorithms, known as post-quantum cryptography. These algorithms are designed to be secure against both classical and quantum attacks, ensuring the longevity of digital security in a future where powerful quantum computers may exist.

The work of Chinese researchers in advancing quantum annealing techniques for integer factorization is an important step in the evolution of quantum computing and cryptography. It reflects ongoing global efforts to understand the capabilities and limitations of quantum technologies.

However, it's crucial to approach claims of breakthroughs with a critical eye.

"We should apply common sense," said Duncan Jones, Head of Cybersecurity at Quantinuum, a leading quantum computing company. "If you were the Chinese military and you had just broken AES, media coverage wouldn't be on your priority list. Instead, you would maximize your informational advantage, without revealing you've broken a critical global cipher."

While incremental advances are being made, they do not currently threaten the security of RSA encryption as used in real-world applications. The challenges of scaling these methods to practical key sizes remain significant.

As the field progresses, staying informed about genuine advancements without succumbing to sensationalism will be key. Collaboration between the scientific community, industry, and policymakers will ensure that we navigate the quantum future with both enthusiasm and caution.

17. A Blueprint for Canadian Deep Tech Leadership from Quantum Industry Canada

by Kyle Briggs
https://docs.google.com/document/d/1NH-SmEfqBFjW2JEl7JSNjeDxkEIkgLIm/edit

Introduction

I recently had the opportunity to interview Lisa Lambert, CEO of Quantum Industry Canada, on the state of quantum technologies in Canada. I have had an eye on this space for a while now, as it is an outlier in Canadian deep tech sectors in that Canada is actually leading globally in many respects.

My goal in this interview was to understand how this came about, and to understand whether Canada's path to its leading position in quantum technologies could be replicated in other deep tech sectors.

This one is by necessity a long post - your email client will probably truncate it before you get to the key takeaways at the end, so be sure to read the web version if you want to get the whole story. Many thanks to Lisa for the detailed and thoughtful responses!

Interview with Lisa Lambert

Kyle Briggs: Tell us about quantum technology generally. What are the promises and potential applications of quantum technology that are driving its development?

Lisa Lambert: *Let's start with quantum mechanics, which is the science of how things behave at the tiniest scales and where the rules of everyday physics that we're used to no longer apply. We've been studying this for 100 years now—we're coming up on the 100th anniversary in 2025, which the UN has declared the International Year of Quantum Science and Technology. But we're now at a point where we've figured out how to really harness quantum mechanics to build some technologies that were never possible before.*

This is really quantum technologies 2.0. The first quantum revolution — quantum technologies 1.0 — we take for granted, as our whole world relies on quantum technologies 1.0. Our GPS system, for example, relies on our initial fundamental understanding of quantum mechanics and is used basically throughout the world. Lasers, MRI imaging, nuclear energy, and transistors are other examples of this. There are more, but we're moving to a new era within quantum and what our capabilities are, which is really exciting. We're now entering the second quantum revolution, where we can actively create, manipulate, and measure quantum states of matter. This new era, often leveraging the quantum effects of superposition and entanglement, is moving beyond theoretical physics into the engineering stage of practical applications.

Canada is a forerunner on the research and commercialization side of this second quantum revolution. We had some early strategic investments on the research side, both public and private investments that have catapulted Canada to a global leadership position. We actually vaulted quantum computing into the commercial arena as well. I'll talk about that a little bit more in a second, but first I want to clarify a common misconception about quantum technologies.

A lot of people, if they know about quantum, might know quantum computing and think that's the only quantum technology. But there are different types of quantum technologies, and Canada has strengths in the research and development of many of them. Among these there's quantum computing, both hardware and software (sometimes called algorithms in the field), which uses the principles of quantum mechanics to process information in new ways, tackling complex problems unreachable by the computers we use today (what we call classical computers). There's quantum communications and networking, which seeks to offer enhanced data transmission security with quantum mechanics and it's working towards creating ultra-private communication networks with significantly improved protection for sensitive business information. Related to this is a technology called post-quantum cryptography (PQC), which is in and of itself not quantum, but involves using some fancy mathematical tools to enhance our cybersecurity to be resilient to an attack from a

quantum computer. And then we've got quantum sensing and imaging, which seeks to provide unmatched precision in measurement and detection, and enables different advancements in fields everywhere from healthcare diagnostics, environmental monitoring, to navigation systems.

Going back to quantum computing, it aims to tackle some complex problems that are currently beyond the reach of today's computing. Potential applications include everything from supply chain optimization, to financial modeling, to material simulation, to drug discovery, to far more. We've got some ideas as to what that will do, but what's most exciting is as this technology continues to evolve, we're going to learn a whole wide range of things that we don't yet know now for what the possibilities are, just like we've learned as we've developed and deployed traditional computing, wireless communication, the internet, and other technologies.

I mentioned earlier that Canada vaulted quantum into the commercial arena. Canada is home to the first commercial quantum computing company, which was founded 25 years ago: D-Wave back in 1999. We also launched the quantum software industry, with 1QBit being the first player in that space, founded in 2012.

If you look at what's happening today in the quantum sector, Canada is currently home to the second highest number of quantum startups globally and we lead in quantum companies per capita (source: The Council of Canadian Academies' Quantum Potential report). So we are among the frontrunners in what has become a global race to develop these critical technologies. And if you look at Canadian companies, it's mostly small and medium sized enterprises and they're competing toe to toe with the global technology giants, in a very capital efficient way. They're leading the pack, pushing innovation and pushing the technological edge in this field right now. For example, Xanadu is the first and only startup to date to demonstrate quantum computational advantage. They did it just after Google did without the big resources that Google has. It was Xanadu's pandemic project to do so, and their software development kit, PennyLane, is one of the leading SDKs in the world. Nord Quantiqueis another example of a Canadian quantum SME pushing the frontiers of what's possible. They are a startup out of Sherbrooke, Quebec, and they're the first company to build a logical qubit beyond break even, which is really key technological achievement for error correction, which is one of the biggest challenges in scaling quantum computing.

Kyle Briggs: How does Quantum Industry Canada fit into all of all of this?

Lisa Lambert: *Quantum Industry Canada, or QIC for short, is the premier industry-led national consortium that unites quantum technology companies and allied organizations with the goal of propelling this sector forward for the benefit of Canada. Our mission is to translate Canadian quantum capabilities and strengths into global business success and national prosperity. So, QIC is focused on the commercialization piece, not just continuing Canada's tradition of being really strong on the research side, but addressing the question of how we capitalize on our knowledge and turn it into an engine for the Canadian economy going forward and harnessing the fullness of Canada's quantum potential.*

Our consortium is expanding quite quickly. We're working with about 70 organizations across the country right now, most of those being Canadian-controlled SMEs. We have three main core goals.

First, we're looking at how to support Canada's quantum industry in achieving global commercial success while enhancing economic prosperity for Canada. Some of that's facilitating access to key resources and opportunities, and a lot of it involves building the road in front of us, tackling common challenges facing our companies. So I often think about, "How do we better identify and address some of the key gaps, blockers, and friction points that are getting in the way of developing Canada's quantum industry and how do we figure that out together?" Even amongst competitors, there are a lot of common gaps and blockers, and we can get farther by working together to address them, especially systemic challenges. Moreover, standing up a new industry is a team sport, and it's crucial for us to collaborate with stakeholders beyond just the quantum and enabling technology companies, but also governments, early adopters of these technologies, investors, the research community, etc.

"Build" is our second core goal: How do we develop early commercial pathways for our industrial base here in Canada and globally? How do we nurture and expand the ecosystem through networks and strategic partnerships? While Canadian companies need to think globally from the outset, they also want to be close to their customer base. That can help retain companies and IP in Canada while spurring innovation in a wide range of sectors applying these new technologies. The thing is, we know traditionally in Canada our business landscape is usually not the early adopters of leading-edge tech, which makes it challenging to build up new deep tech sectors like this one in Canada. So stimulating domestic procurement and adoption is something that is top of mind, while we also work to build bridges across borders.

Our third core goal is to promote and inform. It's important to raise awareness and to showcase Canada's quantum capabilities and the growth opportunities that are emerging from the commercialization of quantum technologies. In Canada, we're a bit modest sometimes, and this can be to our detriment. When it comes to quantum, we have been a global powerhouse. So at QIC, we think about how we can fly that flag and do a better job celebrating our achievements, while recognizing the importance of not letting up and even enhancing our commitment to realizing the full potential of this sector to shape a prosperous Canada where we are at the forefront of the quantum economy.

It's also super important to be a trusted source of information in a sector that can feel a little bit opaque to people and where it can feel challenging to understand where and how to get started. So, QIC aims to help serve as a reliable compass. For us it's important that we are a source of trusted and credible information that people can rely on. Every emerging sector has its share of hype, and we work on cutting through that hype, ensuring that stakeholders have a trusted partner they can turn to to understand the state of these emerging technologies and how these technologies might impact them so they can plan accordingly and move forward with becoming quantum-ready.

Kyle Briggs: Tell me a bit about yourself and how you ended up leading Quantum Industry Canada.

Lisa Lambert: *I was first exposed to quantum 15 or so years ago, when I took up a role at the Perimeter Institute for Theoretical Physics, which was a close collaborator of the University of Waterloo's Institute for Quantum Computing (IQC).*

Prior to that, I was working at the Council of Canadian Academies (CCA), which convenes independent expert panels to analyze and interpret the best available knowledge on complex, pressing issues in a range of policy areas of importance to Canadians.

In my first week on the job at Perimeter, I had the opportunity to visit IQC and learn more about what they're up to firsthand. My host was Raymond Laflamme, a world-renowned quantum scientist, co-founder of IQC, and now serving as the co-chair of the Quantum Advisory Council to Canada's National Quantum Strategy. Ray was very patient with me, and I remember walking into the lab and seeing what looked like these giant beer kegs all over the place. Ray pointed out that these were in fact quantum computers. These were the absolute cutting edge at that time, and the pioneering work to unlock this new technological frontier was happening here in Canada. I was in awe. It was incredible.

It's a bit wild to think back only about 15 years to those early machines and what was the bleeding edge at the time. It was not that long ago and we've come leaps and bounds since. If you look at what Canada's quantum computing companies are working on today, the machines I saw at IQC years back are primitive by comparison. During my time at Perimeter, I had the privilege of working closely with IQC and some of the leading quantum scientists at both institutions, and I was captivated by their work. It was so fascinating to see through what felt like a window into the future.

After that, I moved to Vancouver to join the leadership team at TRIUMF, Canada's particle accelerator centre. I worked there for a number of years and was exposed a bit more to tech transfer through the lab's spinoff companies and commercialization arm. I found the complexities of the journey from lab to market to be quite interesting.

The particular intersection between science and society piqued my curiosity, and stitched together my learnings from a few other experiences, including (1) my work on a report at the CCA titled Innovation and Business Strategy: Why Canada Falls Short; (2) my involvement in launching the Waterloo Global Science Initiative (WGSI) and its first summit Energy 2030 which involved a global exploration of how cutting edge science and technology could advance a sustainable future; (3) as well as my commitment to level up my business acumen, which led me to work with entrepreneur and author Seth Godin and a global team on what was at the time a very forward-thinking approach to equip business leaders with critical skills like leadership, strategy, decision-making, sales, and marketing.

When I was deciding on my next career move, I chose to go into innovation consulting, working mostly with science-based tech companies and taking on a number of other projects that were really interesting to me and gave me a chance to make a significant contribution while learning from some exceptional people.

Quantum was coming up in some of my work, which gave me a lens to see how far the field had come in the last few years. A lot of the researchers that I worked with were now CEOs or leaders of trailblazing quantum technology companies. My curiosity led me to consider how I might be able to bring some of my skillsets together to help advance this nascent industry.

The timing worked out well as it coincided with the CEO opportunity at QIC. I successfully went through the recruitment process and have the privilege of now leading the organization and working with some of the most ambitious, enterprising, and inspiring innovators I've ever known.

Kyle Briggs: As you mentioned before, Canada is among world leaders in quantum technology, which makes it somewhat unique among deep tech sectors. What combination of factors can you identify as being the key to catalyzing and building that leadership position?

Lisa Lambert: *There's been a number of key ingredients that when combined have gotten us where we are today.*

Our early start was instrumental, and quite visionary. Engagement from the public sector at all levels of government has been instrumental in driving this forward, as has investment from the private sector over the years.

Today, we're in the process of reaping the rewards of foundational research investments made decades ago. So we've done a great job of nurturing a vibrant research landscape for quantum in Canada.

Related to this is our leadership in training highly-skilled people in this sector. Workforce development is a hot topic and quantum right now, given the demand for talent as the industry grows. Our estimate is that there are currently a little over 2600 people working in the quantum industry in Canada. A study commissioned by the National Research Council of Canada (NRC) a few years ago projected that Canada's quantum sector will create over 220,000 jobs and contribute to over 3% of the country's GDP, including direct, indirect, and induced impacts. That is a significant growth trajectory for this sector, and one of the key dependencies is people – and it's important to note that most don't require a graduate degree.

Another factor is that Canada has served as the classroom to the world for quantum. For example, the Institute for Quantum Computing, which is today the world's largest quantum computing research centre, was one of the first to offer dedicated graduate programs for quantum and a summer school for undergraduate students, in addition to outreach programming. Being one of the first out of the starting blocks led to a period where about one third of the global quantum workforce had a touch point with IQC. That's shifted now, as more quantum programs have launched across Canada and around the world, but it's an impressive testament to our early foresight and leadership in this sector.

Canada is also home to programs like the Creative Destruction Lab (CDL). I don't know if this is still the current figure, but there was a time where upwards of one half of quantum startups globally had gone through CDL.

For some of them, going through CDL and being exposed to Canada's quantum scene led them to want to partner with Canadian companies and even set up an international office here.

Multiverse Computing, a Spanish-based company and the biggest quantum software company in Europe, is a good example of this.. Their first international office was established in Toronto because of the potential they

saw in the ecosystem when they were in the CDL program, from talent, to partners, to potential adopters, to access to the US market. Their Canadian office provides a strong strategic position for them, and also offers a welcoming environment with many parallels to European culture.

Another critical factor comes down to the boldness, resilience, and ambition of Canada's quantum entrepreneurs. The journey of building a deep tech company in Canada is not for the faint-hearted. Nevertheless, our entrepreneurs are rising to the challenge and striving to build world-class companies while also working together with the QIC community to redefine what it means to build a deep tech company in our country. They're tackling the inherent complexities of quantum technologies while also addressing the unique challenges of building and scaling frontier technology companies in Canada. Their collective efforts are not just building individual companies, but strengthening the entire Canadian quantum industry.

While the combination of these key factors have gotten us to where we are today, it's crucial to recognize that what got us here is not going to get us there.

There is a perpetual issue in Canada where we've struggled to translate our research excellence into value creation, economic growth, and prosperity for our country. If we want to chart a different path for Canada moving forward, we need to better understand and address what's behind this issue.

As we herald a new industry that Canada helped pioneer, we must learn from our past experiences in sectors where we lost our initial lead. It's crucial that we make strategic choices to leverage our early quantum technology advantages effectively. We need to create an environment where our homegrown quantum and enabling technology companies can thrive. This approach will foster a globally competitive industry in Canada that retains talent, develops and protects intellectual property, attracts investment, and translates our research excellence into long-term economic benefits for our nation.

As we consider Canada's future and our innovation landscape, we face crucial questions: Are we content being the world's back office R&D shop for advanced technologies that we pioneered, with our primary export being talent? Or do we aspire to move up the value chain and fully capitalize on our innovations? We must decide how to leverage our strengths to maximize the long-term benefits for Canada's economy and society.

We must decide soon if we want to chart a different course for quantum. Many countries worldwide have rapidly accelerated their focus and investment in quantum technologies, deeming them essential for both economic prosperity and national security. What got us here won't keep us at the forefront of the next leg of the global quantum race. If we stay the course we're on, we risk falling behind and missing out on the immense opportunities this revolutionary technology offers.

As I reflect on this pivotal moment where we decide Canada's role in our quantum future, I can't help but think about Taiwan's strategic approach to semiconductors, which transformed that nation's future. Quantum presents that kind of potential for Canada. We have significant advantages, particularly in the enabling technologies crucial for quantum development. Our strengths span across telecom, photonics, nanofabrication, microelectronics, cybersecurity, and post-quantum cryptography, to name a few. These

sectors, many of which have connections back to our historical telecom industry, have converged to create a unique and powerful quantum ecosystem in Canada.

The next few years are critical as the global community recognizes the industrial opportunities in quantum technologies. We must leverage our diverse technological strengths and act decisively to maintain our competitive edge in this rapidly evolving field.

Kyle Briggs: You mentioned earlier a couple of key early investments that really catalyzed things. Tell me a bit more about that.

Lisa Lambert: *I'll start by sharing one that I'm most familiar with because I was privileged to be part of that journey.*

The Perimeter Institute for Theoretical Physics was envisioned in 1999 by Mike Lazaridis, Co-Founder and then Co-CEO of Research In Motion (RIM), now BlackBerry. Recognizing that much of today's technology—from computers to GPS, wireless communications, and diagnostic imaging—stemmed from breakthroughs in theoretical physics, Lazaridis donated $100 million, one-third of his fortune at the time, to establish a world-leading physics institute. This may still be the largest philanthropic investment in basic research in Canadian history.

In 2002, Lazaridis followed this by founding the Institute for Quantum Computing at the University of Waterloo. Both the provincial and the federal governments at the time stepped up and invested too, along with additional private donors. These initiatives created the backbone for what has become known worldwide as Quantum Valley in Waterloo Region, the first of its kind. Only in recent years have we begun to fully appreciate the scope of Mike Lazaridis' vision, reminding us that ambitious projects require investment, collaboration, commitment, and patience to bear fruit.

Toronto and Ottawa have also been important scenes in Ontario for the development of Canada's quantum strengths and capabilities over the years.

Beyond that, there's been catalysts in a few other key regions across Canada. This year marks the 40th anniversary of BB84, which was co-developed by Canadian Gilles Brassard at the Université de Montréal along with Charlie Bennett, and is the first quantum cryptography protocol. Alexandre Blais and Christian Sarra-Bournet have been driving forces for the sector at the Institut Quantique at the Université de Sherbooke, and now there is Distriq, the Quantum Innovation Zone in Sherbrooke, which is helping to accelerate what has become a globally recognized ecosystem. Elsewhere in Quebec, Montreal, Bromont, and Québec City are home to leading researchers and companies in quantum and enabling technologies.

Moving west, Barry Sanders has been a driving force in Calgary, Alberta over the years, and we're now seeing new public and private investments to develop a global quantum solutions hub in Calgary as well as to advance foundational research in quantum in Calgary, Edmonton, and Lethbridge. In BC, early research led to the spin out of D-Wave from the University of British Columbia and the founding of 1QBit. UBC is also home to the Blusson Quantum Matter Institute, which works with a number of industrial players, and Simon Fraser

University has a number of strong research programs, which helped to attract Stephanie Simmons who founded the quantum computing company Photonic.

This isn't exhaustive, but you can see the narrative emerging of what is a really beautiful story for Canada having a visionary, long-term view that harnesses regional strengths for the development of transformative technologies and a new sector. It's an ambitious endeavor that takes collaboration and time, stretching far beyond an election cycle.

Kyle Briggs: You mentioned earlier that Canada has the highest per capita density of quantum startups in the world. What it is about the quantum ecosystem that enables those startups to get through the valley of death. Why are so many able to continue to exist in Canada where so many other deep tech sectors struggle?

Lisa Lambert: *They're still striving to get through the valley of death. It's important to realize that different quantum technologies have different pathways and timelines to commercialization.*

We have companies that are selling products and services today. These are mostly companies focused on enabling technologies and post-quantum cryptography solutions.

Another tech that's coming into the market is quantum sensing. Canada is home to quantum sensing companies like SBQuantum, that currently offers a quantum-sensing solution for the mining industry.

So some quantum and quantum-related offerings are in the marketplace today, while others require a longer term view to their development and commercialization cycle. This is especially true when it comes to building what's called a "universal fault tolerant quantum computer," which is a quantum computer at a scale that can be useful for business applications. But just because a technology takes some time to develop doesn't mean there's no need for urgency in taking thoughtful actions to accelerate progress and prepare businesses for the quantum era. In fact, I'm more concerned that we won't be ready when quantum technologies reach maturity, failing to recognize their far-reaching implications.

I'm blown away by the ambition and the resourcefulness of our quantum entrepreneurs in this country. They're incredibly clever in figuring out how to take the next step to get where we need to go, and they've been extremely capital efficient and resource efficient in doing so.

However, there are limits to that efficiency and further investment is needed now so that this sector can not just persist, but thrive in Canada for the benefit of our country.

Procurement is really important, and an area where Canada has faltered. Other countries have been successfully leveraging government procurement as a means to accelerate the development of quantum solutions, and this has many positive knock-on effects for their ecosystems, including helping with the attraction and retention of talent, advancing the TRL levels of key technologies, supporting the development and retention of IP, stimulation of private investment, and more. While other countries have been bolstering procurement initiatives, the Government of Canada has made cuts to key commercialization programs like

Innovative Solutions Canada (ISC). While the ISC program is not without its flaws, it's been an important initiative for the country's homegrown quantum sector. The QIC community provided input into the Government of Canada's recent consultations on legislated procurement targets, so we'll see what comes of that.

Kyle Briggs: On that topic, what are the biggest hurdles that Canada needs to overcome to deliver on the promise of quantum technologies beyond the basic research?

Lisa Lambert: *One of the first things is a mindset shift, recognizing that yes, this sector is still in its nascent stages, but there is an industry that's emerging and we've got to start looking at what that industry needs to mature and thrive, and how to address those needs in a way that keeps pace with the development of the industry.*

Canada's National Quantum Strategy (NQS) was a good starting point, but the commercialization pillar is underdeveloped and urgently needs considerable strengthening. In the two years since its launch, the global quantum landscape has evolved rapidly, with significant technological advancements. Other countries are now making substantial investments in their quantum sectors that far surpass the NQS's $360 million commitment from Budget 2021, which was largely allocated to existing programs.

We must recognize that what brought us to our current position won't secure our lead in the next phase of this global race. There needs to be a shift in mindset to acknowledge that we now have a burgeoning quantum industry, not just a research field. This shift should reflect that significant R&D occurs within companies, not just academic institutions.

To advance Canada's quantum sector, we need pragmatic, tailored solutions that acknowledge our unique position. We can't emulate the US or EU approaches, but we can leverage our strengths.

We need to ensure Canada's quantum sector has access to the capital needed to get across the valley of death. Early stage capital is important, and so is patient capital at later stages to enable companies to scale and stay Canadian as they do so. We currently have very few vehicles to this effect, and the time to address this is now.

Government procurement is crucial, but our current system isn't optimized for innovative technologies or Canadian startups. This is not just specific to quantum, but something we're seeing across innovative sectors. While changes to procurement are necessary, they will realistically take time to implement, and we need immediate actions.

That's why it's also important to look at other avenues that are crucial to delivering on the promise of quantum technologies. We could implement new commercialization programs to stimulate adoption in the private sector by derisking early adoption of Canadian quantum technologies by Canadian industry. This approach would provide Canadian companies with customers, push product development, and de-risk private investment.

We must also consider the geopolitical aspects of quantum technology. As a dual-use technology with national and economic security implications, understanding and securing the quantum supply chain is critical. We should take strategic action to position Canada as an integral part of the global quantum market, working closely with trusted allies.

By leveraging our quantum expertise, we can significantly contribute to NATO's technological edge. This approach also offers an innovative way to make headway towards honouring Canada's 2% GDP commitment to NATO, aligning our defense spending with cutting-edge innovation. Furthermore, we should seriously explore joining AUKUS, which can be another pathway to enhancing our quantum capabilities while strengthening our position among key allies. Such partnerships would not only advance our quantum sector but also reinforce Canada's role in shaping global security and technological innovation, ensuring we remain at the forefront of this critical field.

By taking these steps, we can ensure Canada remains a leader in the quantum revolution, leveraging our unique strengths and addressing our specific challenges. Moreover, we can bolster our international standing, contribute meaningfully to global security alliances, and position ourselves at the forefront of strategic technological partnerships. This approach not only advances our quantum sector but also reinforces Canada's role as a key player in shaping the future of global security and technological innovation.

Kyle Briggs: How can Canadian public and private sectors most effectively support quantum companies in addressing all of this? You said what we've done to this point won't get us where we need to go. What do we need to be doing differently going forward?

Lisa Lambert: *Now is the time to engage with quantum technologies. We were late with AI, and we can't afford to repeat that mistake. Quantum will be disruptive, and it's challenging to predict its full impact.*

Some quantum technologies are already here today, with others progressing more rapidly than many anticipated.

In quantum computing, we're seeing roadmaps converge among major players, with initiatives like DARPA's Quantum Benchmarking Initiative expected to accelerate progress. It is hard to predict these things, but if current trends continue, we could see business-relevant quantum computers within the next decade, with some experts saying this could be sooner.

I encourage everyone to get curious and start engaging and considering how quantum technologies might impact you. QIC publishes a monthly newsletter called "Quantum Eh?", is a great resource to stay informed about the sector. Connect with quantum companies to explore potential applications in your industry. QIC can help make introductions to relevant players or we are happy to work with groups to host roundtables to explore this frontier technology (here is a summary of a roundtable with a cross-section of members from the Canadian Chamber of Commerce). What I'm excited about is that quantum offers real opportunities for innovation and to stimulate innovation, not just within the quantum technology companies themselves, but across all industries. Ultimately quantum is a tool that's going to be applied across all different sectors.

In 2025, QIC is hosting QUANTUM NOW, in partnership with Distriq and Québec Quantique. This is going to be Canada's first industry-led quantum tech forum, and it's aimed at prospective adopters, policymakers at all levels of government, and investors. It's designed to help people understand and navigate the quantum landscape, giving them a shorthand or heuristic to think about this transformative technology sector as it moves forward, and building connections with Canada's leading quantum innovators.

I'm proud of Canada's quantum sector, but the story isn't finished. We need help writing the next chapter. Let's bring quantum into broader conversations about innovation, economic growth, and national security. This isn't just about technological advancement; it's about securing Canada's future prosperity and sovereignty in an increasingly complex global landscape. We'd be happy to participate in these crucial discussions, as quantum has the potential to benefit all Canadians while strengthening our nation's economic and security posture.

Kyle Briggs: When you consider recent policy shifts, for example the cuts to Innovative Solutions Canada, the proposed changes to SR&ED, overhaul, and what is looking less and less like an overhaul of IRAP, how do you anticipate these will impact the Canadian quantum ecosystem?

Lisa Lambert: *The recent policy shifts are already impacting the quantum ecosystem. Stability and predictability in the policy landscape are crucial for deep tech sectors, especially quantum. Sudden changes or retractions introduce volatility, affecting both companies and investors' confidence.*

The cuts to Innovative Solutions Canada (ISC) were particularly challenging, as ISC was part of the National Quantum Strategy's commercialization pillar announced in 2023. This program was crucial as it provided not only non-dilutive capital but also gave companies a customer through government procurement. For quantum companies, this dual benefit was invaluable. Losing ISC means losing both funding and a potential early customer, which is a significant setback for many startups in the sector.

Regarding SR&ED, we've provided input for both consultation rounds (you can view the recommendations developed by a QIC Working Group here and here). It's been a key program for deep tech development in Canada, including quantum, and there are opportunities to modernize it to drive more innovation and long-term value. We're optimistic about potential improvements, such as factoring in IP and equipment purchases.

IRAP has some great people working on quantum, and we're grateful for their support and thoughtfulness in considering the role IRAP can play in advancing this critical sector.

The announcement and subsequent withdrawal of the Canadian Innovation Corporation (CIC) was disappointing. There was considerable excitement and anticipation surrounding this initiative, as it was designed to address critical gaps in our innovation ecosystem. I found Danny Breznitz's input in shaping this initiative to be particularly insightful and on point. CIC was expected to address current gaps, which now remain open. It's crucial that we find alternative ways to address these gaps promptly. The quantum sector, along with other deep tech areas, requires consistent, thoughtful support to maintain Canada's position as a global innovator and to translate our research strengths into economic advantages.

I firmly believe that modern economies will be built on advanced technologies, with quantum being a prime area of opportunity. Canada has been a frontrunner in research and early-stage development. Our challenge now is to avoid self-imposed obstacles and transform our quantum strengths and capabilities into engines of prosperity for our nation. We must address the issues that are getting in the way of effectively leveraging our quantum innovations to drive economic growth, create high-value jobs, and secure Canada's position as a global leader in this critical sector.

Key Takeaways

Canadian leadership in quantum technologies holds key lessons that generalize to other sectors of deep tech. It did not happen spontaneously, but rather represents the combination of four key ingredients: a deep pool of highly trained talent, the existence of infrastructure to enable that talent to push the research forward, visionary leadership that was willing to make a bet that may not pay off during their tenure, and a catalyst event that seeded what became a virtuous cycle of innovation. The catalyst in this case was a series of investments made in quantum technologies in the Waterloo region that led to the establishment of the Perimeter Institute. This investment was made decades ago, at a stage when quantum technologies generally were still firmly in the realm of academic research.

In the case of quantum technologies, it was the vision of an individual who made a massive philanthropic investment that set Canada on its path to dominance. However, relying on once-in-a-century good will is not a valid strategy for deep tech development. The good news is that there is no obvious reason that the catalyst needs to come from a private individual. Examples abound globally of similar virtuous cycles of innovation catalyzed by public sector investments. If Canada hopes to achieve a similar position of leadership in other deep tech sectors, our policy makers will need to step up and provide that catalyst deliberately.

The failure of the Canadian public sector to learn this lesson leads to other challenges that were identified in the interview: not only are we the world's source of intellectual property, but we are the world's schoolhouse, training and exporting a steady stream of world-class talent.

Canada has many sectors that have three of the four key ingredients: deep talent pools, world-class research infrastructure, and world-leading minds are common across many deep tech sectors in Canada, but without a national vision for what results from these raw ingredients to focus them toward a long-term goal, Canada rarely gets past the stage of filing academic IP. What separates these sectors from quantum is the catalyst, the visionary investment made before the potential impact was obvious. Without these in other sectors, Canada will continue its century-long trend of being an IP and talent republic, content to produce innovative technologies and brilliant researchers on behalf of the rest of the world.

Also of note in the quantum story is the scale of investment required. While Mike Lazaridis' investment and subsequent public sector follow-on was a massive expenditure for an individual, it was relatively small (on the scale of hundreds of millions) relative to the amounts that are being poured into AI today. Canada's budget 2024 has allocated $2.4B for AI infrastructure investments, nearly an order of magnitude more than what was required to set Canada on the path toward global quantum dominance, but given the decades-long delay in

committing relative to the same point in quantum development, Canada's AI investments will barely move the needle, representing less than half of that which will be spent by a single American company this year (OpenAI is projected to spend $5B). In spite of the fact that ISED proudly boasts that Canada has 10% of the world's top AI talent, Canada may have missed its opportunity to be relevant in AI by many years due to underinvestment in the early stages.

***In other words:** waiting until we are sure that a technology will work means missing the opportunity to benefit. This is especially true for a small economy like Canada. While giants like the US and China can afford to come late to the party by simply throwing vast resources at the problem, we cannot. On the other hand, investing early means that a much smaller investment is needed to achieve impact. If Canada hopes to benefit from its research excellence, the public sector needs to embrace risk and invest in technologies when they are still in their nascent stages, trading the uncertainty over which bets will pay off for the opportunity to be first mover in those that do, to ensure that talent, infrastructure, and vision are concentrated here before the rest of the world catches up.*

Finally, it is necessary to stay the course, and recognize that the level and form of support needed is not a static thing across the lifecycle of a deep tech sector. While Canada leads in quantum technologies for now, the hard work of Quantum Industry Canada and other private sector supports for early commercialization efforts of quantum and quantum-enabling technologies remains essential in carrying Canada across the finish line. From the recent policy-induced whiplash relating to procurement cuts, delays to the CIC, and Canada's underinvestment relative to China, more directly comparable countries like Netherlands, and even Singapore, it is likely that without this hard work, our public sector innovation leaders would drop this ball, too.

The silver lining is that challenge is also opportunity. While Canada may well have missed its chance in AI, the productivity of our national research machine means that technologies abound that could be the next disruptor. The last few decades of quantum technologies provide a clear blueprint for how to achieve deep tech dominance that can be readily replicated in other sectors, while the current trajectory of Canada's AI development is well on its way to being a blueprint for how to lose it. It is incumbent on Canadian policymakers to learn from these examples to finally address Canada's failures in translating research excellence into long-term economic impact.

18. Most Organizations Unprepared for Post-Quantum Threat

by Beth Maundrill
https://www.infosecurity-magazine.com/news/orgs-unprepared-postquantum-threat/

Despite NIST's recent publication of post-quantum encryption standards, many organizations have not begun preparing for the post-quantum threat, according to a new report by the Entrust Cybersecurity Institute.

In August, NIST published its first three finalized post-quantum encryption standards, outlining usage and implementation guidelines for organizations entering a new era of quantum cryptography.

While 36% of organizations globally favor implementing a strict post-quantum cryptography (PQC) plan, a significant proportion are inclined towards a hybrid approach (31%) or initial internal testing of PQC (26%), Entrust found through its survey of over 2,000 IT security experts' attitudes to PQC.

Entrust said that its findings on PQC and public key infrastructure (PKI) showed that less than half of organizations are preparing, and more than one-third lack the necessary scale or technology to transition to PQC.

"There's a shift in the industry with regard to post-quantum readiness," said Samantha Mabey, Director of Digital Solutions Marketing at Entrust. "While the questions around the post quantum threat used to be 'is it real', the questions as of late are now 'what do I need to do' and 'how'."

Significant Barriers to Quantum Cryptography Transition

The *2024 PKI and Post Quantum Trends Study* found that ownership, skills and inconsistent requirements serve as the top challenges for enabling applications of PKI.

It also said that 51% of respondents reported a lack of clear ownership over this transition.

Another challenge was visibility of cryptographic assets, with 43% of organizations citing an inability to simply inventory their crypto assets.

"Organizations know that the threat of post quantum is inevitable and impact substantial, but they lack the cryptographic visibility, skills and computing power needed to effectively activate a plan, revealing a critical gap between awareness and action as the quantum threat looms. A major focus for organizations in 2025 will be activating these plans, bolstering their visibility into their cryptographic assets, and preparing their teams for a quantum-safe future," said Mabey.

Entrust's 2024 PKI and Post Quantum Trends Study presents findings from a survey of IT and IT security professionals across the US, UK, Canada, Germany, UAE, Australia/New Zealand, Japan, Singapore and the Middle East, conducted by the Ponemon Institute.

19. Google's 67-Qubit Sycamore Quantum Computer Could Beat Top Supercomputers: Study

https://www.gadgets360.com/science/news/google-sycamore-quantum-computer-67-qubit-outperform-top-supercomputers-study-6775585

Recent advancements in quantum computing have revealed that Google's 67-qubit Sycamore processor can outperform the fastest classical supercomputers. This breakthrough, detailed in a study published in Nature on October 9, 2024, indicates a new phase in quantum computation known as the "weak noise phase."

Understanding the Weak Noise Phase

The research, spearheaded by Alexis Morvan at Google Quantum AI, demonstrates how quantum processors can enter this stable computationally complex phase. During this phase, the Sycamore chip is capable of executing calculations that exceed the performance capabilities of traditional supercomputers. According to Google representatives, this discovery represents a significant step towards real-world applications for quantum technology that cannot be replicated by classical computers.

The Role of Qubits in Quantum Computing

Quantum computers leverage qubits, which harness the principles of quantum mechanics to perform calculations in parallel. This contrasts sharply with classical computing, where bits process information sequentially. The exponential power of qubits allows quantum machines to solve problems in seconds that would take classical computers thousands of years. However, qubits are highly sensitive to interference, leading to a higher failure rate; for instance, around 1 in 100 qubits may fail, compared to an incredibly low failure rate of 1 in a billion billion bits in classical systems.

Overcoming Challenges: Noise and Error Correction

Despite the potential, quantum computing faces significant challenges, primarily the noise that affects qubit performance. To achieve "quantum supremacy," effective error correction methods are necessary, especially as the number of qubits increases, as per a LiveScience report. Currently, the largest quantum machines have around 1,000 qubits, and scaling up presents complex technical hurdles.

The Experiment: Random Circuit Sampling

In the recent experiment, Google researchers employed a technique called random circuit sampling (RCS) to evaluate the performance of a two-dimensional grid of superconducting qubits. RCS serves as a benchmark to compare the capabilities of quantum computers against classical supercomputers and is regarded as one of the most challenging benchmarks in quantum computing.

The findings indicated that by manipulating noise levels and controlling quantum correlations, the researchers could transition qubits into the "weak noise phase." In this state, the computations became sufficiently complex, demonstrating that the Sycamore chip could outperform classical systems.

20. Canada's Quantum Leap: A Call to G7 Leadership

by GQI
https://quantumcomputingreport.com/canadas-quantum-leap-a-call-to-g7-leadership/

The International Council of Quantum Industry Associations (ICQIA) is urging Canada to prioritize quantum technologies during its 2025 G7 Presidency, seeing it as a pivotal opportunity to solidify global leadership in this transformative field.

Why is this Important?

- Quantum technologies are essential for economic prosperity and national security. The ICQIA highlights that other G7 nations and security alliances are rapidly increasing their focus and investments in this area, such as NATO with its billion dollar innovation fund and the AUKUS Framework.

- 2025 is a landmark year for quantum. The UN has declared it the International Year of Quantum Science and Technology, and Canada will host the inaugural QUANTUM NOW / ICI QUANTIQUE forum in Montreal (June 18– 19th 2025). This convergence of events creates a perfect stage for G7 discussions on quantum advancements. And it is GQI's opinion that the ICQIA should use this to facilitate conversation between G7 members and industry leaders. Perhaps utilising members of industry bodies or leaders in the fields with focused discussions on how quantum can impact SDGs (societal development goals)

What are the key calls to action?

The ICQIA proposes that Canada spearhead global action in the following areas:

- Enhanced cooperation among G7 nations to position them as leaders in the quantum revolution.

- Harnessing quantum solutions to address global challenges like energy-efficient AI and achieving Sustainable Development Goals.

- Strengthening quantum supply chains and fostering talent pipelines to build enduring quantum capabilities across G7 nations

- Leveraging quantum technologies to bolster economic growth and address national security concerns, reinforcing the G7's global influence.

This message carry's significant weight behind it, with the ICQIA representing nearly 600 stakeholders across the international quantum innovation ecosystem, standing ready to support Canada in this endeavour.

A letter sent by ICQIA to Canadian Prime Minister Justin Trudeau urging him to take this under consideration can be accessed here.

21. NATO's Quantum-Safe Future Transition

by GQI
https://quantumcomputingreport.com/natos-quantum-safe-future-transition/

A Jewel Buried Deeply

Buried inside of nineteen policy statements that describe the organization's goals for quantum technology in general terms, are five surprisingly, specific, references to Post-Quantum Cryptography.

And buried inside of one set of bullet points, for the general item #4, is the most surprising bullet point of all:

- NATO has identified, understood and capitalised on evolving quantum technologies advancements, including with enabling technologies and in convergence with other EDTs;
- NATO has a Transatlantic Quantum Community to strategically engage with government, industry and academia from across our innovation ecosystems;
- NATO has transitioned its cryptographic systems to quantum-safe cryptography;
- Relevant quantum strategies, policies and action plans are dynamically updated and executed; and
- Allies have become aware of, and act to prevent, on a voluntary basis, adversarial investments and interference into our quantum ecosystems, which can include, on a national basis, the examination of relevant supply chains.

After sorting out the tenses (Did they already transition? No, it is in progress.), we suggest to watch NATO closely. It will be the first multinational government organization to undertake this task. You can see their desired goal from their press from only two years ago. Here they have tried one element in 2022, of a secure VPN, one baby step towards the full solution. Since NIST released on August 13, 2024, their final, approved specifications for the first three PQC algorithms, NATO has now a set of PQC protocols to work quickly. There is a 'Q-day' worst case scenario, coming up.

To understand how massive this feat is, NATO consists of 32 member countries, 5 million active + reserve military personnel from all member states, 30+ major military bases and command centers, with many smaller facilities across each NATO member state.

In our observation of this feat in progress: who in NATO, and which NATO division to undertake the task? The process could be a model for PQC adoption in other large, multinational organizations, for example: the U.N.. I'll leave this as an open question to be answered in the future.

GQI's Perspective for a Quantum Safe Future

For the most resilient strategy against 'Q-day', the day that current cryptographic protocols are broken (worst case scenario says 2027), GQI advises a multi-layered approach, the easiest might be first with PQC, which is math-based, and joining with Quantum Key Distribution (QKD), which is physics-based. From GQI's 77 page, *Quantum Safe Outlook Report*:

GQI believes that crypto-agility will be a long term requirement for the new cryptographic stack. For the most sensitive applications, particularly those where a long security shelf-life is an ongoing requirement, a layered defense-in-depth should be considered.

As the world sets-out on the transition to quantum-safe cyber security, the obvious first port of call are new quantum-resistant math-based cryptographic algorithms. NIST has been leading international efforts to establish standards for such post-quantum cryptography (PQC).

These techniques are being joined by other physical security options. These include new techniques for out-of-band key delivery, and an array of techniques from quantum cryptography (notably QRNG, and QKD). These are best viewed not as an alternative to math-based security, but as new complementary tools. When correctly designed and implemented, these can offer additional unique properties and a further strengthened security promise. Whether these tools bring additional complexity or welcome flexibility is hotly debated. So too is in what situations they represent a good investment of the security budget.

22. Chinese Scientists Report Using Quantum Computer to Hack Military-grade Encryption

by Matt Swayne

https://thequantuminsider.com/2024/10/11/chinese-scientists-report-using-quantum-computer-to-hack-military-grade-encryption/

Chinese scientists have successfully mounted what they claim is the world's first effective attack using a quantum computer on widely used encryption methods, according to a report from the South China Morning Post (SCMP). The researchers did acknowledge that limitations would hamper – at least for now – a full-on quantum hack.

The advance, led by Wang Chao of Shanghai University, poses a "real and substantial threat" to the security mechanisms used in banking and military sectors, as detailed in their peer-reviewed paper published on September 30 in the *Chinese Journal of Computers*, an academic journal run by the China Computer Federation (CCF).

Despite the general-purpose quantum computing field still being in its early stages, with no immediate risk to modern cryptographic systems, scientists are increasingly exploring specialized quantum computers for potential uses – and, in the case of cybersecurity, vulnerabilities. In their recent study, Wang's team utilized a quantum computer from Canada's D-Wave Systems to breach cryptographic algorithms, marking a significant milestone.

According to SCMP, the research team employed the D-Wave Advantage quantum computer to target the Present, Gift-64, and Rectangle algorithms, called key representatives of the Substitution-Permutation Network (SPN) structure. This structure is foundational for advanced encryption standards (AES), a system widely deployed in military and financial encryption protocols, according to the newspaper. While AES-256 is often labeled as military-grade and considered the most secure encryption standard available, the study suggests that quantum computers may soon threaten such security.

"This is the first time that a real quantum computer has posed a real and substantial threat to multiple full-scale SPN structured algorithms in use today," Wang's team wrote. Given the sensitivity of the research, Wang declined to provide further comments to SCMP.

The D-Wave Advantage, initially designed for practical applications rather than cryptographic attacks, has been previously used by a range of companies and organizations to explore tasks in logistics and finance, for example. SCMP reports that the machine employs a technique known as quantum annealing, which simulates a process similar to metallurgy where materials are heated and cooled to increase strength. This method allows the computer to rapidly solve complex mathematical problems.

The principle behind quantum annealing involves searching for the lowest energy state, akin to guiding a ball through a landscape filled with hills and valleys. Traditional algorithms must explore every path, climbing and descending multiple times. However, quantum tunneling – an effect where particles pass through barriers rather than over them – enables the quantum computer to find the lowest point more efficiently, bypassing obstacles that classical methods cannot.

Wang's paper described this technique as similar to an artificial intelligence algorithm capable of optimizing solutions on a global scale. His team combined the quantum annealing algorithm with conventional mathematical approaches to create a novel computational architecture. The significance of Wang's work, according to SCMP's anonymous expert, lies in framing a real-world encryption issue as a binary optimization problem suitable for a quantum computer.

Despite this achievement, the researchers acknowledged the current constraints of quantum computing technology. In the report, Wang stated that while quantum computing shows promise, its development is

hampered by environmental factors, immature hardware and the challenge of devising a single attack algorithm capable of breaching multiple cryptographic systems.

The study emphasizes that while a quantum computer has not yet revealed the specific passcodes used in the algorithms tested, it is closer to doing so than previously achieved. As the technology advances, the researchers suggest that further developments could yield more robust quantum attacks. The ongoing evolution in quantum computing points to potential new vulnerabilities in existing cryptographic systems as scientists push the limits of what these machines can accomplish, SCMP reports.

23. Encryption backdoor debates rage across the planet, promising a difficult 2025 for CISOs

by Evan Schuman
https://www.csoonline.com/article/3555354/encryption-backdoor-debates-rage-across-the-planet-promising-a-difficult-2025-for-cisos.html

The European Union is now arguing various versions of encryption backdoor rules, but they are not expected to agree on much. Their members, though, are likely to each create their own contradictory rules.

Compliance rules requiring encryption backdoors – not just for attachments, but for text; not just for communications apps, but mobile devices, clouds, and SaaS apps – are being hotly debated in just about every corner of the planet.

Although much of the compliance community is focused on European Union debates right now, encryption companies are just as concerned with legislative efforts in Australia, which is seen as likely to be the first country fully embracing encryption backdoors. Canada, Japan, and various other countries are also considering such moves, along with some legislators in the United States.

But in Europe, the lack of agreement among EU member countries, in addition to the UK, will likely mean that those countries will create their own encryption backdoor rules, with no attempt to make the rules consistent, either in terms of requirements or in penalties for non-compliance.

"We are looking at a diverse panoply of [encryption] laws across countries, regions, and states," said Brian Levine, an Ernst & Young (E&Y) managing director overseeing cybersecurity strategies. "This is a matter of balancing safety versus security, and remembering that they are not the same thing and there is value to both."

A steamy mess

A more blunt assessment came from Audian Paxson, the principal technical strategist for Ironscales, an enterprise cloud email security company.

The encryption backdoor global compliance situation in 2025 will be "a big three-dimensional hot steamy mess, and it's a joke. It's also going to be, to a certain degree, futile," Paxson said. "The feasibility for the countries in the EU to come together is unrealistic. And fragmented laws don't have a lot of teeth."

For enterprise CISOs, this issue will be tricky. These compliance regulations will not have direct jurisdiction over enterprises, but they will have a potentially massive secondary effect. The rules will directly apply to the vendors that enterprises contract with for everything from messaging apps to cloud environments, mobile devices, VPNs, SaaS platforms, and potentially even IoT and IIoT devices. Anything that can transmit data may be caught in the regulatory maze by at least some of these geographies.

The CISOs need to protect all manner of sensitive and restricted data, especially in highly-regulated verticals such as healthcare and finance, along with aerospace and others who might have government or military contracts requiring security clearances.

These backdoor rules will generally require some employees or contractors of that vendor to have unlimited access to the unencrypted version of all transmissions. That is so that those workers can then share the files with law enforcement.

The risk for CISOs is either that one of those vendors or law enforcement workers is untrustworthy and steals or sells that data, or that the vendor or law enforcement body is breached and the data gets into the open that way.

"It's always hard to prevent the bad actions of a privileged insider," Levine said.

CSAM argument is flawed

The key talking point of legislators arguing for encryption backdoors is that it will attack things such as child pornography, known in encryption circles as CSAM (child sexual abuse material).

Many in cryptography find that argument to be flawed. "Scanning files for CSAM and comparing those hashes to hashes of known CSAM is not an effective way to limit this form of illegal content because most CSAM is new content," said Augustine Fou, an independent cybersecurity researcher who is about to offer his own enterprise B2B encryption app. "Child abusers want new CSAM content, not old ones, so comparing to known hashes does not reduce illegal activity."

Paxson agreed, adding that the child pornographers will quickly move out of regulated environments, either to the dark web or various private encrypted channels. "All of the good guys will try to play by the rules, but the criminals they are targeting will simply move to their decentralized encryption," Paxson said. "The criminals will react faster than everybody else. The attackers are smart enough to go to quantum level encryption."

E&Y's Levine, a former prosecutor with the US Justice Department, disagreed with both points. Levine argued that the entities that collect these hashes, primarily the FBI and the National Center for Missing and Exploited Children, are collecting new images and files constantly and adding them to their databases. "They have the known hash value of all of that child porn. These databases are being updated every day," he said.

More critically, Levine said, the fact that these criminals will move off the public platforms to the dark web or their own private environments is precisely the goal. Although the criminals will continue to create and sell their files, they will be separated from their child victims and will therefore be unable to groom them into making such videos or photos. "That's the point. These kids aren't on the dark web" or in private environments.

Georgianna Shea, the chief technologist at the Foundation for Defense of Democracies, which calls itself a nonpartisan think tank focused on national security and foreign policy, said that the likely patchwork of new encryption backdoor rules will become almost-unworkable for enterprise CISOs.

"I am not going to continually re-architect based on an infinite number of standards that crop up," Shea said, adding that she expects CISOs to "start tagging data to remove European information."

Her biggest concern is losing control of highly confidential data. "Someone has to look at that image. Who is looking at it? Who gets access to it? How does that impact your customers who have given that trust to you?" Shea said, asking what happens if the data does get into the wrong hands. "Did you just lose that customer if they end up suing you? Is China going to end up with your secret formula? What is at fault there? What are the access controls? The adversaries, the bad guys, always find a way around it."

Richard Blech, CEO of encryption company XSOC, said the encryption backdoor compliance efforts "are not feasible or practical at all. Once the door is open, the door is open to everybody. Australia is heavily pushing toward some kind of backdoor or at least the ability to eavesdrop. They may be the first to break through, long before anyone in the EU even gets close," Blech said.

One approach for enterprise CISOs is to create their own secure communication channels with customers and business partners in impacted geographies, Blech said, for example, using an enterprise-grade VPN to tunnel into a secure area in the enterprise's on prem environment. Then all communications could theoretically be protected.

That is, he added, "just as long as the VPN itself does not have a backdoor. There have been some discussions with AES having some vulnerabilities there."

One major encrypted messaging app, Signal, has already discussed plans to help customers steer clear of these pending encryption backdoor rules. "Signal provides a built-in censorship circumvention feature and also includes support for a simple TLS proxy that can bypass these blocks in many circumstances and let people communicate privately," said a Signal blog post.

Signal did not reply to a message left by CSO to comment on the post.

Blech, after reading Signal's blog said: "Yeah, they probably didn't talk to their lawyers about that. But with the initiative taken, the legal aspects notwithstanding, it seems to be a workable approach."

24. A New Phase for Quantum Competition in Europe

by David Shaw
https://quantumcomputingreport.com/a-new-phase-for-quantum-competition-in-europe/

Political renewal is evolving priorities in Europe, inside and outside the EU. The opening of IBM's first Quantum Data Center in Europe signals a new phase in quantum competition. Speaking at the launch of the new center, Olaf Scholz issued a rallying cry for those focused on building a quantum future based on collaboration and competition rather than national silos. How does Europe stand in the quantum race?

The Need for Growth

The vagaries of short term hype cycles aside, a wave of new technologies stand poised to define 21st century economies. The list varies: AI, quantum, bio-engineering, autonomy, space technologies and advanced materials typically figure prominently. Collectively known as deep tech, the technical uncertainties and potentially long timescales surrounding their development make these challenging areas, for policy makers and for investors.

Neither does the economic backdrop provide simplification. Deglobalization has seen a rise in economic nationalism. The challenge of climate change remains depressingly difficult to grasp. Geopolitical tension is increasingly spilling over into real regional conflicts. Migration is a political flash point.

Against this backdrop, countries in the West fear their economic lead is slipping, and traditional engines of growth are stalling. There is also no real consensus on policy responses. Can industrial strategy reignite a constructive spiral, or will it descend into destructive protectionism? Should it focus on supporting key technologies (see list above) or pursue more societal missions (specific objectives in climate, security or the environment)? How can the animal spirits of capitalism be harnessed to support this journey? Not just in funding startups, but also in intelligently steering the substantial funds needed to fund the scale-up of these technologies?

European countries in particular are waking up to the imperative of technology innovation to drive growth in an otherwise aging continent that simultaneously faces the major imperatives of decarbonisation and improving security. In a sweeping report on 'The future of European competitiveness', Mario Draghi has called for €800B per annum increased investment and a new innovation focussed industrial strategy for the EU. This envisages increased central EU coordination to mobilize the programme, ideally stimulated with new jointly issued EU debt. Elsewhere in Europe, Keir Starmer's new UK government has identified growth as its own number one objective.

There are headwinds. Cautious Northern Europeans have traditionally resisted the direct EU borrowing that might fund major new investment. In some countries, those on the right retain a suspicion of industrial strategy, as a doomed attempt to 'pick winners'. Even traditional champions like France find their current budgets constrained. In Germany, ever since the constitutional court's decision to tightly interpret the country's constitutional 'debt brake', Olaf Shultz' coalition government has struggled for internal alignment and public popularity.

The Quantum Opportunity for Europe

What role can quantum technology play in helping Europe meet its ambitions? The promise here is strong. Based directly on our most fundamental science, quantum holds unique potential as a new general purpose technology, able to deliver impacts across a wide array of applications and industry sectors. It is naturally well positioned to support objectives in clean energy, better health, security and an improved environment. Crucially, Europe has real strengths.

Europe is the original home of quantum theory and boasts many strong academic institutions active in cutting edge research. It is strongly represented in many end-use industries that are ultimately expected to benefit from quantum technologies. In 2014, the UK (then still part of the EU) launched the world's first national quantum program, The EU later launched its own €1B Quantum Flagship initiative in 2017 (set to run for 10 years); a clutch of national initiatives followed in other member states. EU programs such as Horizon Europe, EuroQCI, EuroHPC and more recently the EU Chips Act have sought to promote joint action (and significantly expanded spending). Beyond the EU, the European Space Agency (ESA) provides a natural focus for space elements. QuIC as an industry association is increasingly prominent in providing industry participants with their own voice.

However, challenges remain. After 2021, the technology-led flagship focus of Horizon 2020 was not carried forward to Horizon Europe, which instead was oriented around societal missions. The Quantum Flagship continued, but perhaps lost some of the prominence it might have enjoyed. Achieving real coordination across national quantum programs has also been elusive. Resources can seem spread thin across national interests rather than providing focus and scale. Multiple centers are being propped-up in national and regional competition to host nascent ecosystems. ESA illustrates the most extreme version of this, where geographical return rules means funds must be spent in proportion within each contributing nation.

Other policy objectives have also been at play. A consistent theme has been the EU's desire for technological sovereignty: avoiding dependence on supply chains outside its borders, both in China and the US. This has been combined with what has increasingly seemed an antagonistic relationship with US Big Tech. The EU has sought to exploit its ability to lead on regulation, but many consider its recent initiatives on AI to simply hinder rather than guide the development of this important new technology within its borders.

Much has been written about the effects of Brexit on the UK. In the domain of quantum technology the reverse is also evident. Britain's absence from Horizon Europe severely depressed collaboration with many

strong UK institutes. The UK boasts 4 universities in the world top 10, all with leading quantum tech research activities, The UK quantum program, now in its 10th year, is the world's most mature and unarguably a great success. London, though facing its own challenges, remains Europe's most credible and deepest capital market. The continuing exclusion of the UK from terrestrial Horizon Europe quantum work programmes, even after the UK obtained associate country status, can only be interpreted as flowing from the hardest of lines on technological sovereignty. A lack of ambition for collaboration with the US likewise.

Other factors have started to act as a counterweight to these forces pulling apart Western collaboration. War in Ukraine has focussed European governments again on the need for collective security. NATO has been active in promoting quantum initiatives across member states: including the DIANE quantum accelerator, hosted by Deep Tech Lab in Denmark, the NATO Innovation Fund and most recently the proposed Transatlantic Quantum Community.

Many leading nations have implemented export controls on quantum technologies, including the US, UK, Germany, France, Canada, Japan and Australia. Though in practice this doesn't yet seem to have impacted trade between traditionally friendly countries.

.
.
.

25. Research team develops hardware architecture for post-quantum cryptography

by Falko Schoklitsch
https://techxplore.com/news/2024-10-team-hardware-architecture-quantum-cryptography.html

Integrating post-quantum security algorithms into hardware has long been considered a challenge. But a research team at TU Graz has now developed hardware for NIST post-quantum cryptography standards with additional security measures for this purpose.

They are not yet a reality, but in the not-too-distant future, sophisticated, high-performance quantum computers will be available. They will revolutionize fields like artificial intelligence, financial modeling, drug development, weather forecasting, and traffic optimization, but they also pose a significant risk to cybersecurity.

A powerful quantum computer will break a subset of widely used cryptographic algorithms that are important in securing the digital world. This is why several quantum-safe, more commonly known as "post-quantum cryptography" (PQC) algorithms, are already being developed. Implementing them into hardware has proven difficult so far, though.

In the PQC-SRC project, a team led by Sujoy Sinha Roy from the Institute of Applied Information Processing (IAIK) and Communications at Graz University of Technology (TU Graz) has developed hardware for these PQC algorithms and implemented additional security measures. During the research, the team was also in contact with companies such as Intel and AMD.

The work is published in the journal *IEEE Transactions on Computers*.

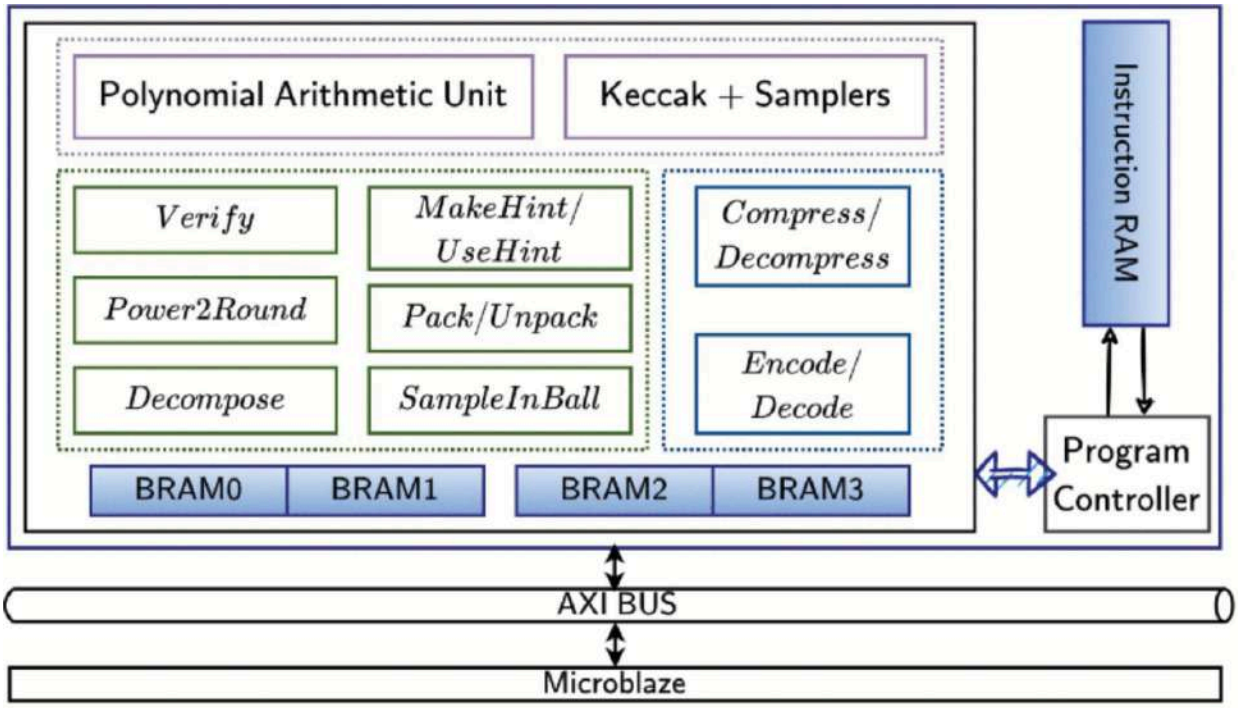
Among the algorithms, those based on computational problems involving mathematical lattice structures are particularly promising. Solving these computational problems is considered an infeasible task even for quantum computers.

In the process of standardizing PQC, the American National Institute for Standards and Technology (NIST) selected one key encapsulation mechanism (KEM) algorithm, namely Kyber, and three digital signature algorithms, namely Dilithium, Falcon, and SPHINCS+, which was partly developed at IAIK, for standardization.

KEM algorithms enable communicating parties to agree on the same encryption key securely, while digital signature algorithms allow a receiver to verify the authenticity of received messages.
Need for secure and efficient design

Following the publication of standardized PQC algorithms, organizations and industry are gearing up for a transition to quantum-safe cryptography. All devices need to switch from classical KEM and signature algorithms to quantum-safe PQC algorithms. It becomes imperative that the newly standardized PQC algorithms be realizable on a wide range of electronic devices.

There is an urgent need for secure and efficient design and implementation methodologies to enable a smooth transition to quantum-safe cryptography. Researchers of the Cryptographic Engineering team, led by Sujoy Sinha Roy, have been researching such methodologies, especially targeting low-resource electronic devices. The PQC-SRC project has resulted in the development of several new methodologies.



Development of hardware-based coprocessor for standardized PQC

One research result is the construction of a unified cryptographic coprocessor named KaLi, which supports both Kyber KEM and Dilithium digital signature algorithms. Such a unified design is essential in real-life secure communication protocols, such as the widely used Transport Layer Security (TLS), where both KEM and signature operations are performed.

One main research challenge was how to make the unified design very compact. The new PQC algorithms require much larger memory and processing units to store and process the keys compared to the present-day ones. If the design is not compact, a lot of low-resource computers used in IOT, and smart-card applications will be rendered inoperable.

Another important aspect is the agility or flexibility of architecture—minor changes to the cryptographic algorithms due to potential future threats can be accepted without replacing the hardware resources.

Besides efficiency and compactness, a cryptographic implementation's physical security is important. Although the mathematics behind a cryptographic algorithm may resist known mathematical attacks, the physics of a computing device might leak sensitive information in the form of variations in heat, radiation or energy consumption.

An attacker can try to guess what is happening within an electronic device using an antenna. The researchers investigated techniques to make cryptographic implementations of emerging PQC algorithms resistant to such attacks. They invented a data randomization technique named "Kavach."
The technique optimizes the computation overhead, taking special properties of numbers used in the polynomial operations of PQC algorithms. The results will help cryptographers construct PQC KEM and signature algorithms that are more friendly to countermeasures against physics-based attacks.

Important step for companies and organizations

"We have seen great leaps in the field of quantum processors over the past five years," says Sujoy Sinha Roy.

"When powerful quantum computers are fully developed, they will be able to break encryptions in a few seconds, for which conventional computers would take years. This would be dangerous for banking transactions, state defense systems and other things. This is often referred to as the quantum apocalypse and we want to prevent it.

"As companies and organizations prepare to move to post-quantum cryptography, our research findings provide an important step towards this transition."

26.IonQ Demonstrates Remote Ion-Ion Entanglement, a Significant Milestone in Developing Networked Quantum Systems at Scale

by Tyler Ogoshi
https://investors.ionq.com/news/news-details/2024/IonQ-Demonstrates-Remote-Ion-Ion-Entanglement-a-Significant-Milestone-in-Developing-Networked-Quantum-Systems-at-Scale/default.aspx

IonQ, a leader in the quantum computing industry, announced it has achieved the next milestone on the path towards scaling its quantum systems – demonstrating remote ion-ion entanglement. Building off the ion-photon entanglement achievement announced in February, this demonstration announced in September showcases the second out of four significant milestones required to develop photonic interconnects – a foundational step towards quantum networking and a core component of IonQ's scaling strategy.

IonQ's world-class R&D team entangled two trapped ion qubits from separate trap wells using entangled photons to achieve these results. The IonQ team achieved remote entanglement by developing a system to collect photons from two trap wells and routing them to a single detection hub. This critical "point-to-point" step established a quantum communication link – an essential piece in scaling quantum systems. While IonQ has always intended to implement photonic interconnects in

its systems, never before has any company demonstrated the ability to bring this technology to an integration stage within a commercially available, enterprise-grade quantum computer. More details about IonQ's latest milestone are available in the blog post here .

"IonQ's north star remains scalability at high performance, and the progress we've made towards photonic interconnects ensures our customers will have access to large quantum systems capable of tackling the most complex problems," said Peter Chapman, President & CEO, IonQ. "We're consistently making significant headway on our technical roadmap, and customers across academia and business recognize the unique value IonQ's systems bring as we near the point of commercial quantum advantage."

"IonQ's unique architecture and technology relies on scaling qubits within a single ion trap and then networking multiple traps together to achieve commercial quantum advantage," said Dr. Björn Flatt, Head of Emerging Technologies, IonQ. "With our latest achievements, we are now focused on the next phase for achieving scale – swapping ion-ion entanglement to the QPU. We are committed to pushing the boundaries on this technology and bringing photonic interconnects to a technical readiness where they can be integrated in commercially available quantum computers."

IonQ is making rapid progress on its journey towards unlocking massive scale via modularity and photonic interconnects. IonQ has made technological and architectural choices by embracing a practical path that balances three core pillars required for commercial advantage: Performance, Scale, and Enterprise-Grade capabilities. Governments, global business enterprises, and academic institutions worldwide trust IonQ to deliver fast, accurate, and accessible quantum computers that open new opportunities for every industry.

27. D-Wave Introduces Service-Level Agreements for Leap Quantum Cloud Customers in Production

by Alex Daigle

https://www.dwavesys.com/company/newsroom/press-release/d-wave-introduces-service-level-agreements-for-leap-quantum-cloud-customers-in-production/

D-Wave Quantum Inc., a leader in quantum computing systems, software, and services and the world's first commercial supplier of quantum computers, today announced the introduction of service-level agreements (SLAs) specifically tailored for Leap™quantum cloud service customers who are transitioning applications into production. By establishing formal SLAs, D-Wave stands behind the high levels of availability, reliability and scalability of its Leap cloud service and its ability to support requirements for commercial-grade quantum and hybrid-quantum applications as customers move into production deployments.

The Leap quantum cloud service—providing real-time, secure access to D-Wave's annealing quantum computers and hybrid solvers since 2018—has proven to be a production-grade service on which customers can run business-critical workflows. D-Wave's monitoring data confirms that the Leap service has consistently exceeded 99.9% availability for its Solver API and its aggregated set of annealing quantum computers over the past two years, meaning that the service is highly responsive even during periods of high demand.

Since the launch of the Leap service, customers have run nearly 200 million jobs without having to schedule work in advance, endure lengthy queue times, or work around unavailable hardware. On average, it takes just a fraction of a second to process a job directly on the QPU, according to recent median sample-time measurements. D-Wave recently introduced enhancements to the Leap service and the Ocean™ SDK that boost its already remarkably fast processing speeds by 30%, enabling customers to achieve even faster computations and solve complex problems more effectively. In the past 12 months, the Leap service has seen a surge in usage, with over 60 million jobs submitted, a 215% increase over the previous 12 months. This growth highlights the demand for immediate access to cloud-based quantum computing, reinforcing D-Wave's decision to create an SLA offering for its customers.

"When it comes to incorporating quantum computing into a company's overall IT infrastructure, organizations should consider prioritizing a real-time production-grade quantum cloud service that offers the kind of assurances that service-level agreements provide," said Heather West, PhD, research manager and analyst with IDC. "Technology leaders should have the same expectations of quantum cloud services that they do for any software-as-a-service, with reliability and accessibility leading their decision criteria."

"As the transition to production deployments accelerates, providing exceptional access to our cloud service has never been more critical," said Dr. Trevor Lanting, chief development officer of D-Wave. "Our SLA offering is designed to support this dynamic shift with confidence, enabling businesses to thrive as quantum technology's commercial value and adoption grows."

28. What Communications Companies Need to Know Before Q-Day

by Aritra Banerjee
https://www.darkreading.com/ics-ot-security/communications-ict-q-day

After a grueling eight years of testing, the National Institute of Standards and Technology (NIST) has finalized the first three algorithms that will form the backbone of the world's strategy to counter the potential threats of quantum computing.

Given that enterprising hackers are likely already harvesting and storing massive volumes of encrypted sensitive data for future exploitation, this is welcome news. We have the first post-quantum cryptography (PQC) algorithms to defend against the inevitable attacks on "Q-Day," when a cryptographically relevant quantum computer (CRQC) comes online.

Still, having these NIST-approved algorithms is just the first step. For the information and communications technology (ICT) industry, transitioning to a quantum-safe infrastructure is not a straightforward task; numerous challenges must be overcome. It requires a combination of engineering efforts, proactive assessment, evaluation of available technologies, and a careful approach to product development.

The Post-Quantum Transition

PQC algorithms are relatively new, and with no CRQC available to fully test, we cannot yet achieve 100% certainty of their success. Yet we know that any asymmetric cryptographic algorithm based on integer factorization, finite field discrete logarithms, or elliptic curve discrete logarithms will be vulnerable to attacks from a CRQC using Shor's algorithm. That means key agreement schemes (Diffie-Hellman or Elliptic Curve Diffie-Hellman), key transport (RSA encryption) mechanisms, and digital signatures must be replaced.

Conversely, symmetric-key cryptographic algorithms are generally not directly affected by quantum computing advancements and can continue to be used, with potentially straightforward increases to key size to stay ahead of quantum-boosted brute-forcing attacks.

Hybrid Approach to Security

The migration to PQC is unique in the history of modern digital cryptography in that neither traditional nor post-quantum algorithms are fully trusted to protect data for the required lifetimes. During the transition from traditional to post-quantum algorithms, we will need to use both algorithm types.

Defense and government institutions have already begun integrating these algorithms into the security protocols of specific applications and services due to the long-term sensitivity of their data. Private companies have also kicked off initiatives. For instance, Apple is using Kyber to create post-quantum encryption in iMessage, while Amazon is using Kyber in AWS.

Large-scale proliferation of PQC is coming, as global standards bodies, such as 3GPP and IETF, have already begun incorporating them into the security protocols of future standards releases. For instance, the IETF-designed Transport Layer Security (TLS) and Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) – two of the most widely used protocols across 3GPP networks– will both incorporate PQC.

This kind of standardization is key for industries like telecommunications and Internet services, where hundreds of different companies are providing the different hardware, device, and software components of

a network. Like any security protocol, PQC must be implemented consistently across all exposed elements in the network chain because any link that isn't quantum-safe will become the focal point of any data harvesting attack.

Over the next few years, we will see more and more PQC-enhanced products enter the market. At first, they will likely use hybrid approaches to security, using both classical and post-quantum encryption schemes, as Apple and Amazon have done. But as quantum-security technologies advance and are further tested in the market, PQC will likely replace classical asymmetric encryption methods.

Because asymmetric algorithms are largely used for secure communications between organizations or endpoints that may not have previously interacted, a significant amount of coordination in the ecosystem is needed. Such transitions are some of the most complicated in the tech industry and will require staged migrations.

Ready for Q-Day

PQC isn't the only way to protect against a quantum attack, as quantum threats will only increase in sophistication. It's vital to deploy a defense-in-depth strategy –- one that includes physics-based solutions like preshared keys with symmetric distribution and quantum key distribution (QKD) – but PQC will be a powerful security tool.

Attention to interoperability will be key here, as crypto agility will ease the migration to pure quantum-safe algorithms in the future. Some companies are already leaning toward open source rather than proprietary code, which can help to avoid a bumpy upgrade path in future for security products. As well, this crypto agility will ensure that technologies being designed now for inclusion in next-generation/6G products will also have backward-compatibility with 5G and other earlier standards.

Now that we have the essential first algorithms to build our arsenal against quantum computing threats, the next steps for the ICT industry will be critical. They must adopt hybrid solutions now to combat harvest-now-decrypt-later attacks; embrace crypto agility, interoperability, and rigorous testing; and deploy a defense-in-depth strategy. By following this strategy, we will be well on track to ensuring our long-term security and saving the world from potential disaster when Q-Day comes.

29.How post-quantum cryptography is reshaping cybersecurity in 2024

by Pascal Brier

https://www.capgemini.com/be-en/insights/expert-perspectives/how-post-quantum-cryptography-is-reshaping-cybersecurity-in-2024/

Last year, we predicted that post-quantum cryptography (PQC) would be a defining technology trend in 2024 with far-reaching implications for organizations.

Following the release of NIST's post-quantum encryption standards a few weeks ago, the race to secure IT systems for the quantum era has accelerated. Nowhere is this urgency more pronounced than in the financial sector, where sensitive data, stringent regulations, and vast datasets demand a rapid shift to quantum-safe systems

As #quantum computing advances, it presents both opportunities and risks for the financial sector. On one hand, quantum computing could revolutionize financial processes such as market trading, risk management, and secure communication through technologies like quantum key distribution. On the other hand, it could create significant exposure, particularly to public-key cryptography, which underpins the security of digital communications. Cyber actors may use quantum computers to break current encryption methods, creating a scenario where sensitive financial data becomes vulnerable. The concept of "harvest now, decrypt later" is particularly concerning, as threat actors might intercept encrypted data today, with the aim of decrypting it once quantum computers mature.

Recently, the G7 Cyber Expert Group published a very interesting statement that highlights the dual nature of this technology.

The G7 is urging financial institutions to start planning for post-quantum cryptography (PQC) as soon as possible to safeguard future communications. Financial institutions are encouraged to assess their own quantum risks, build inventories of vulnerable systems, and implement governance processes to mitigate emerging threats.

Personally, I would go beyond the G7's recommendations and urge organizations across all sectors to start investigating and navigating the complex quantum landscape.

There are many actions that CxOs can take today to start preparing for a quantum future: such as auditing current cryptographic systems, investing in quantum-resistant algorithms, and ensuring that quantum readiness is integrated into long-term IT roadmaps.

Quantum computing is advancing faster than initially predicted, and when it reaches critical maturity, it will be too late to start preparing. Post-quantum cryptography implementation will not be easy, so a gradual migration with careful planning will be essential. Starting now will prevent unwelcome surprises and allow an orderly migration. The actions we take today will determine whether we are resilient or exposed when quantum supremacy becomes a reality.

30. CISA aims for inventory clarity with post-quantum cryptography guidance

by Matt Bracken
https://fedscoop.com/cisa-post-quantum-cryptography-guidance/

The Cybersecurity and Infrastructure Security Agency is pushing forward on its oversight of federal post-quantum cryptography migration, unveiling a strategy document last week that details how the agency intends to monitor and assess governmentwide progress on the transition.

The public release of CISA's guidance on Friday, required by a 2022 Office of Management and Budget memorandum on migrating to post-quantum cryptography, lays out plans for the deployment of automated cryptography discovery and inventory (ACDI) tools to aid agencies as they work to inventory any IT systems or assets that may contain vulnerable cryptography.

The cyber agency said the ACDI tools will serve the purpose of automating "the collection of the cryptographic characteristics required for the inventory," and also be integrated with its Continuous Diagnostics and Mitigation (CDM) program. Combining forces with ACDI tools and the CDM program could lessen the resources needed for generating inventory content, the guidance noted.

Much of CISA's guidance centers on the inventorying of data items that agencies will have to report. Agencies are currently required by OMB to report their inventories through CyberScope, a spreadsheet form that is submitted to CISA and the Office of the National Cyber Director. OMB's memo notes that future changes to Federal Information Security Modernization Act requirements will require updates to CyberScope, but agencies should continue reporting through that system.

CISA's guidance lists multiple steps for how ACDI tools should be developed and integrated, including instructions for how those tools should be added to a list of CDM-approved products, how modifications to CDM dashboards should be handled and more.

The cyber agency has now embarked on "a long transition period" that will see it "monitor and maintain the status of migration to PQC," according to the guidance, while it also continues to observe agency reporting on the use of quantum-vulnerable cryptography and offer support as needed.

Other actions required over the next several months include the creation of a list of PQC-enabled products for cryptographic systems by CISA and the General Services Administration, the publication of an initial draft documenting the National Institute of Standards and Technology's "demonstrations of discovery and inventory tools," and the launch of a CISA-run pilot program on ACDI tool development and integration.

31. IBM algorithms chosen as part of NIST's first post-quantum standards

by Back End News
https://backendnews.net/ibm-algorithms-chosen-as-part-of-nists-first-post-quantum-standards/

The National Institute of Standards and Technology (NIST) has published the first post-quantum cryptography standards, selecting three algorithms to protect data against the future risks posed by quantum computing.

Two of these algorithms, **ML-KEM** and **ML-DSA**, were developed by IBM researchers in collaboration with industry partners. A third, SLH-DSA, was co-developed by a researcher who later joined IBM.
Quantum computers, unlike traditional systems, have the potential to break the encryption methods currently safeguarding data. These new cryptography standards aim to address that concern by creating algorithms that quantum computers cannot easily compromise.

"IBM's mission in quantum computing is two-fold: to bring useful quantum computing to the world and to make the world quantum-safe," Jay Gambetta, VP at IBM Quantum, said in a media release. "We are excited about the incredible progress we have made with today's quantum computers, which are being used across global industries to explore problems as we push towards fully error-corrected systems."

Security concerns

He noted, though, that these advancements could herald an upheaval in the security of most sensitive data and systems. He acknowledged that NIST's publication of their first three post-quantum cryptography standards marks a significant step in efforts to build a quantum-safe future alongside quantum computing.

IBM is actively pushing the development of quantum systems, expecting to deliver its first error-corrected quantum system by 2029. This new technology is expected to handle computations that today's classical computers cannot, solving complex problems across various industries, such as healthcare and logistics.

However, as quantum systems advance, they could become a threat to current cybersecurity standards, like RSA encryption, which has long protected global data. IBM's cryptographic experts have been working for decades to develop solutions, and their algorithms are set to replace existing encryption methods, ensuring a quantum-secure future.

NIST's newly published standards are a key step toward protecting data transmitted over public networks and used for identity verification. The standards provide a framework for governments and industries to begin implementing post-quantum security measures.

32.First IBM Quantum Data Center in Europe Opens

by Erin Angelini
https://irishtechnews.ie/nordvpn-post-quantum-encryption-support/

Alongside German Chancellor Olaf Scholz, senior European government officials and European-based global enterprises, IBM today unveiled the first IBM Quantum Data Center located outside of the United States. It is the company's second quantum data center in the world and marks a significant expansion of its fleet of advanced, utility-scale quantum systems available to global users via the cloud.

Now online in Ehningen, Germany, Europe's first IBM Quantum Data Center includes two new utility-scale, IBM Quantum Eagle-based systems, and will soon feature a new IBM Quantum Heron-based system. These systems are capable of performing computations beyond the brute-force simulation capabilities of classical computers.

First introduced late last year, IBM Heron is the company's most performant quantum chip yet, and advances the company's mission of bringing useful quantum computing to the world by enabling users to increase the complexity of algorithms they are exploring on real quantum hardware.

When the IBM Heron-based system is made available at the IBM Quantum Data Center in Europe, it will be the third IBM Heron installed across IBM's fleet of quantum systems that can be accessed by the company's global quantum network of more than 250 enterprises, universities, research institutions, and organizations. IBM Heron offers up to a 16-fold increase in performance and 25-fold increase in speed over previous IBM quantum computers as they were measured two years ago.

When it is deployed alongside the now-available utility-scale systems installed in the new IBM Quantum Data Center, the IBM Heron-based system will expand the more than a dozen quantum computers IBM currently offers through the cloud – the largest fleet of its kind in the world.

The opening of the new quantum data center was celebrated at a ribbon-cutting event attended by senior government officials, including German Chancellor Olaf Scholz and Dr. Nicole Hoffmeister-Kraut, Minister for Economic Affairs, Labour, and Tourism, State of Baden-Württemberg. IBM CEO and Chairman Arvind Krishna gave remarks alongside Chancellor Scholz, and the Chancellor also spoke at length with IBM leaders including Dario Gil, IBM Senior Vice President and Director of Research; Ana Paula Assis, General Manager of IBM EMEA; Jay Gambetta, Vice President of IBM Quantum; and IBM Quantum's German-based team about the importance of quantum computing's adoption and growth in the region.

Additionally, the landmark moment was attended by several senior leaders of European-based global enterprises, including Crédit Mutuel, Bosch, E.ON, Volkswagen Group, and others, as well as research institutions such as Ikerbasque in Spain and Fraunhofer-Gesellschaft. These organizations are among the more than 80 European-based organizations within the IBM Quantum Network, many of which have the opportunity to access the systems within the IBM Quantum Data Center in Europe to search for the algorithms and applications of quantum computing that could solve some of the most complex challenges across their industries.

"The opening of the IBM Quantum Data Center in Ehningen is good news for Germany. It will serve as a location for innovation and business growth, and is an expression of investors' confidence in the German market. IBM enriches the German quantum computing landscape with this new data center. The German government is providing targeted support for the development of quantum technologies. It is thereby driving forward the development of competencies and capacities in quantum computing in order to promote a robust ecosystem around the development of quantum computers," said Olaf Scholz, Chancellor of the Federal Republic of Germany.

"The opening of our first IBM Quantum Data Center in Europe marks a pivotal moment for the region's technological development, demonstrates our commitment to Europe, and underscores the key role of collaboration with industry, academia and policymakers for a pan-European quantum ecosystem. This state-of-the-art facility will foster innovation around quantum computing, creating new opportunities for talent attraction and ensuring that Europe remains at the forefront of global technological advancements," said Ana Paula Assis, General Manager and Chairman of IBM Europe, Middle East and Africa.

"Our collaboration with IBM for the 'scaling' phase of quantum computing is progressing according to plan. We are working to develop concrete applications that improve the experience of our customers and members, and create value for the Group's businesses," said Frantz Rublé, President of Euro-Information and Deputy Chief Executive Officer of Crédit Mutuel Alliance Fédérale. "The availability of this quantum data center on European soil addresses our constraints in terms of processing proximity and Crédit Mutuel's approach to regulatory compliance. And it also means we can look forward to the next stages of the quantum project with confidence at Crédit Mutuel, CIC and then at Targobank."

"We believe that enabling our scientists and engineers to tackle demanding problems in materials sciences, high-energy physics, and biosciences through quantum computing, and providing state-of-the-art quantum computing access will be key to make disruptive progress in all those disciplines," said Javier Aizpurua, Ikerbasque professor, Donostia International Physics Center (DIPC) and director of BasQ. "A combined use of quantum computing, AI, and data science, if generalized, will give rise to a scenario of new possibilities not only in fundamental research but also in industrial innovation."

"Bosch aims to drive innovation in the field of material simulation using quantum computing. In partnership with IBM Quantum, our team is creating scalable algorithms that aim to revolutionize product development. This includes the creation of new materials for sustainable, carbon-free mobility and the reduction of rare earth elements," said Dr. Thomas Kropf, President of Corporate Sector Research and Advance Engineering, Robert Bosch GmbH. "The European IBM Quantum Data Center allows us to run quantum calculations in close proximity, supporting Bosch's approach to compliance with European data protection regulations. This accelerates our research and development efforts and bolsters the European quantum ecosystem, paving the way for advancements in mobility, healthcare, and sustainable technologies."

"E.ON is investigating quantum computing to tackle energy transition challenges, including large-scale optimization, complex scenario modeling, and quantum machine learning. IBM's first European Quantum Data Center's location is also helpful for EU/German public funding opportunities, which may be available for local access to quantum computational resources and on-site expertise. This milestone underscores Europe's and Germany's leadership in quantum computing and marks a significant advancement in propelling enterprises into the quantum era," said Chris d'Arcy, Managing Director, E.ON Digital Technology GmbH and Chief Data and AI Officer.

"Quantum computing can be the next big thing to solve problems in material science, traffic optimization, or deep learning, that may change the world. IBM's Quantum Data Center in Europe provides access to their unique quantum infrastructure and thus, represents an indispensable another piece of the bridge between quantum computers and industrial application at scale. We are proud to be part of that journey to utilize quantum computing for the transformation into future sustainable and smart mobility," said Dr. Nikolai Ardey, Executive Director, Volkswagen Group Innovation.

"Algorithmiq is pioneering the integration of quantum computing, artificial intelligence (AI), and network science to solve the world's most complex problems in chemistry, healthcare and life sciences. To accomplish this, we need algorithms and scale. This is why we've partnered with IBM on both counts: our groundbreaking error mitigation algorithm, TEM, available through the Qiskit Functions Catalog, is proven to be optimal in extending the scale and accuracy of quantum simulations. And now, with more IBM quantum systems available in Europe, we're excited to further strengthen our ties in Europe and partner with an even larger ecosystem of industries, organizations, developers, and scientists to demonstrate TEM's utility – and progress toward quantum advantage," said Sabrina Maniscalco, CEO of Algorithmiq.

IBM recently published evidence that Qiskit is the world's leading and most performant quantum software. Together with access to IBM's advanced quantum hardware, IBM's ecosystem of users across Europe and globally can access tools and systems that can help them to more easily advance the discovery of algorithms that could open the doorway to useful quantum computing and reach quantum advantage: the point at which a quantum computer can solve a practical problem better than any classical method.

The IBM Quantum Data Center in Europe can be accessed through the IBM Quantum Platform, continuing IBM's mission to enable the development of quantum computing use cases and to support clients as they press forward with algorithm discovery in the era of quantum utility, and towards quantum advantage.

33.NordVPN Launches Post-quantum Encryption Support for First Application

by Irish Tech News
https://irishtechnews.ie/nordvpn-post-quantum-encryption-support/

Starting with quantum-resilient encryption support for the Linux application, NordVPN aims to implement post-quantum cryptography for all applications.

NordVPN, a leading cybersecurity company, launches its first VPN application with quantum-resilient encryption. The first iteration of post-quantum cryptography support for **NordLynx** is now available on the NordVPN Linux application. Additionally, the company plans to implement post-quantum algorithms on all NordVPN applications by 2025 Q1 at the latest.

"Trends show that cybercriminals are intensifying what are known as 'harvest now, decrypt later' attacks. Simply put, they are trying to accumulate huge quantities of encrypted data and decrypt them once quantum technology is developed. Thus, the VPN industry must enter a new phase of development to defend against future quantum computing threats. With this launch, we start a major transition to new generation encryption of all our applications, providing long-term security for our users," says Marijus Briedis, CTO at NordVPN.

The recent announcement by NIST regarding the first post-quantum cryptographic standards is significant for the VPN industry as it signals the beginning of a necessary transition to quantum-resistant encryption methods. VPNs rely heavily on cryptographic protocols for securing communication, so the industry must now prepare to adopt these new standards to ensure long-term security against future quantum computer threats.

The rollout of the NordVPN Linux application with the first iteration of post-quantum cryptography will allow the company's team of engineers to gather essential performance data, including its impact on connection times and speeds. Based on these insights, NordVPN aims to extend post-quantum cryptography support to all of their applications by 2025 Q1 at the latest.

Implementing post-quantum encryption in a VPN presents technical challenges. While security remains paramount, ensuring that post-quantum algorithms are performant enough for real-world deployment is equally critical. These algorithms typically require much larger key sizes and signatures than traditional ones, leading to increased computational overhead, which can negatively impact VPN speed and performance, particularly in high-throughput environments.

"These technical challenges are the reason for the gradual implementation of post-quantum cryptography support to our applications. We want to be completely sure that we will keep the highest level of user experience in terms of connection time and speed during the transition," Briedis says.

Moreover, NordVPN aims to ensure that applications are both quantum-resistant and agile in cryptographic management. As cryptographic needs evolve, the demand for crypto-agility that enables systems to adapt to new cryptographic standards seamlessly will be essential.