Crypto News

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

June 01, 2024

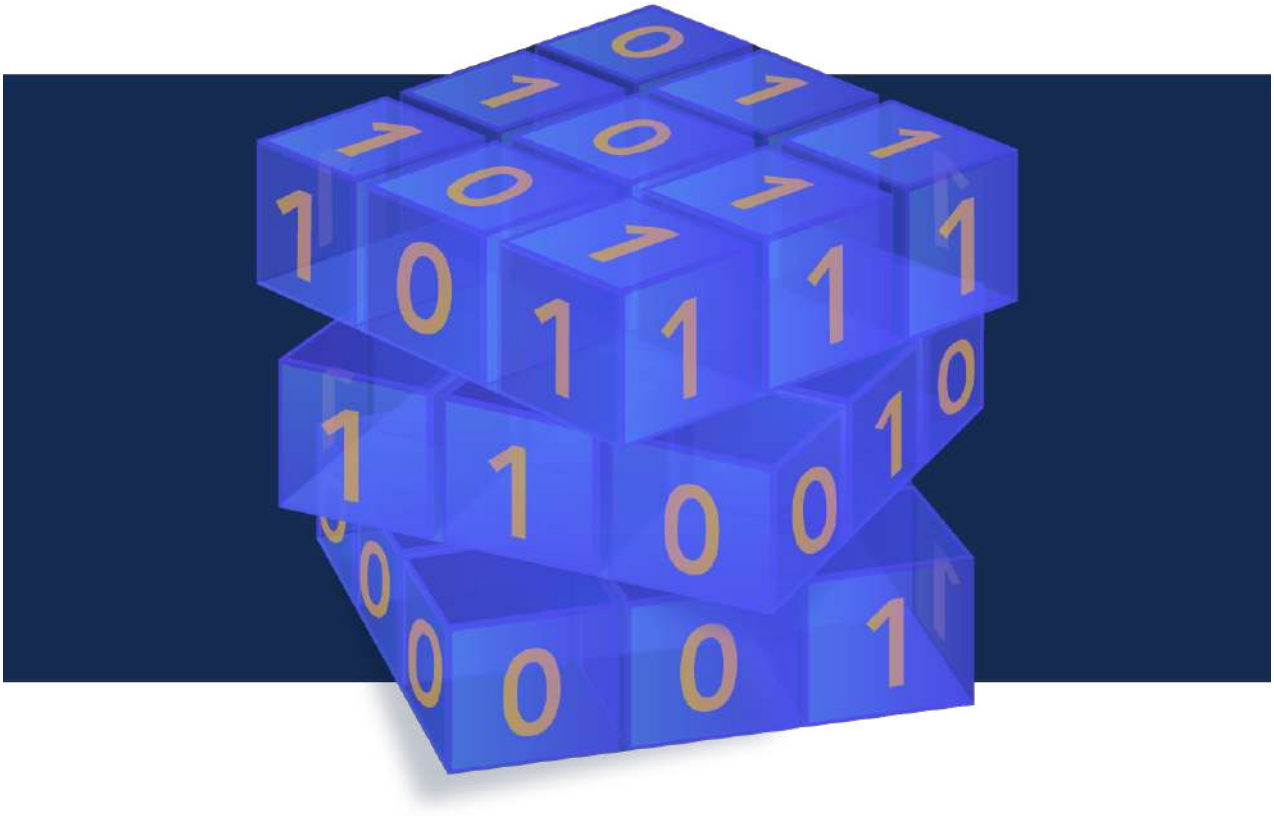


TABLE OF CONTENTS

Editorial

Happy summer readers! For those who weren't able to make it to RSA this year, you'll want to get an update on what was discussed about our quantum future in article 19. It's encouraging to hear that we are past the awareness stage of the quantum threat with those in the technology and cybersecurity fields and organizations are thinking about what to do next. It's further encouraging to hear that this forward thinking isn't confined to just the finance, big tech, and telecommunications industries but is seeping into the retail and the automotive industries as well. The topics discussed at RSA were around PQC standardization, hardware efficiency challenges, PQC adoption strategies, legacy system compatibility, and export control of PQC solutions. This is in addition to vendors who were there bringing awareness and solutions for organizations to consider. As a friendly note from this author, organizations need to remember to vet potential vendors based on the organizations business and technology needs and comply with their vendor risk management strategies and regulatory requirements rather than hastening to buy a solution that may not be right or right-sized for the organization. This step should be a part of any post-quantum planning at your organization. Even with the progress seen in the technology ecosystem in terms of quantum awareness, it's important to remember that there are still a high number of organizations who have yet to plan, let alone implement those plans and solutions, for their quantum futures. If yours is one of these organizations, I suggest hastening your efforts. For more updates from the RSA conference, navigate to the article to learn more.

Governments are also paying close attention to and rolling out new solutions for organizations to consider and adopt. The highly anticipated release of the NIST post-quantum cryptography standards is rumored to be released in July. Keep an eye out for the finalization of FIPS 203, FIPS 204, and FIPS 205. If you want to learn more about these standards, make your way to articles 8 and 13 as well as the NIST website. The Netherlands is also moving towards securing their infrastructure at a time when critical infrastructure is in the limelight globally. The Port of Rotterdam, a key port for trade in Europe, is going to get an upgrade to their network using quantum technology. For more information about who they're working with to make this happen, scroll down to article 18. As always, there's a number of other interesting articles that you won't want to miss in this issue. Happy reading!

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

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

1.Post-Quantum Cryptography: security implications for the boardroom

by Bill Tanner
https://www.intelligentcio.com/north-america/2024/05/31/post-quantum-cryptography-security-implications-for-the-boardroom/

We can safely assume that most of the top-level executives are aware of quantum computing, especially when 100% of Fortune 500 companies and the majority of Global 2000 companies have a Chief Information Security Officer (CISO) who has certainly done at least a first assessment of the impact of Quantum Computing.

The key conversation now is around securing their organisations against quantum computing threats.

This requires engagement from an entire company. For those operating in certain industries, it could be a costly, lengthy process that involves securing millions of digital assets.

So, what does the rest of the boardroom need to know about Quantum Computing?

It would be difficult to explore the inner-workings of quantum computers in this article without going into the complex, counter-intuitive theory behind them – what most people need to know is that they could be vastly more powerful than conventional computers.

To over-simplify the complex world of digital security, a company's digital assets are protected by mathematics. The long and complex numbers that function as 'keys' to a particular digital lock could take upwards of trillions of years for a standard computer to solve, but they can be solved, and this means that the only thing preventing your digital assets from being open to all is computing power.

'Quantum Supremacy', the point at which a quantum computer can carry out calculations for certain problems faster than a conventional computer, was achieved several years ago. While we are perhaps years or even decades away from a Quantum General Computer, the fact that they could break standard forms of encryption that all digital security relies upon has been known about for years.

The first and most significant point to note in quantum computing is that we don't know when working, commercially available quantum computers will be created. Just as at the quantum level everything is a jumble of shifting probabilities and contradictions, the world of emerging quantum computers is similarly unclear. The systems themselves are being developed by governments and very large corporations such as IBM and Google, so the most up-to-date developments are often behind closed doors and any information in the public domain should always be treated with caution.

Any announcements that a company or government has achieved a new fastest quantum computer do not necessarily mean that we are much closer to working quantum computers. Current quantum computers make one error in every hundred operations, but to be truly useful they would need an error ratio of one in a trillion. Algorithms can be used to compensate for these errors to a point, but to truly correct for them major advances need to be made in the systems themselves – and the problem is so severe that IBM has a ten-year roadmap for developing fault-resistant quantum computers.

That in no way means that usable, fault tolerant quantum computers are guaranteed to arrive in 2034 but does mean that we need to question anyone who claims that it will arrive within the next few years.

I would always encourage all companies to carry out an audit of which of their resources need to be secure (at the very least), but there are industries in which deploying post-quantum cryptography should be a matter of absolute urgency.

Firstly, any company that sells goods with long life cycles. The average car spends 11 years on the road before being scrapped, and a lot can happen in that time.

As a rule of thumb, if a connected device is likely, or even possibly, going to be used for five years or more then you should make sure that it is prepared for quantum cryptography.

For a similar reason, companies that manufacture components used by other companies also need to look at their quantum security.

You won't know how long your components will be in use for, and their end-users may not know or be able to control the way they are secured, so it is best to be safe and protect them now.

Moreover, it is likely that the first instances of harm caused by quantum computing are going to be between state actors, as opposed to smaller cybercrime gangs. In this case, critical infrastructure such as power, water and transport will be the first civilian networks to be targeted – this has been the case for literally decades and will only become more dangerous as states have access to quantum computing.

Similarly, it goes without saying that companies that either work directly with or around the defence industry, not just in their own country but in any, will be prime targets for state-based or aligned bad actors with access to quantum computing.

Finally, regulated entities such as those in financial services and healthcare keep long-term, highly sensitive data on their customers, and if this data is altered -or even could be altered- then this would have major effects on the world's financial environment, which relies on accurate records.

I must make clear that none of the above means that companies that aren't in these sectors are safe – if any company leaves themselves unprotected then various bad actors will, in time, find a way to exploit that, perhaps by decrypting the data much later.

And although there is a great deal of complexity around quantum computing, organisations like NIST have already worked out quantum-safe algorithms to protect data, and hundreds or thousands of companies are already using them to secure their data, even though the threats to that data have not emerged.

In fear of labouring the point, we simply don't know exactly when quantum computing will go from being a hypothetical to a threat, but it's essential that the C-Suites of any and every company, not just the CIO or CISO, start preparing now by assessing what cryptographic assets are in use today that need to be protected against tomorrow's threats.

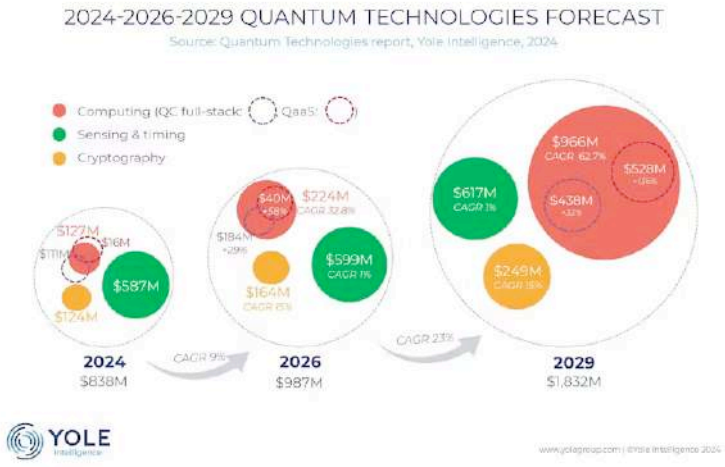
2.Quantum continues to be a buoyant field where photonics will play a critical role

by Eric Mounier

https://www.laserfocusworld.com/quantum/article/55041716/yole-developpement-quantum-continues-to-be-a-buoyant-field-where-photonics-will-play-a-critical-role

Quantum is a strategic technology domain with multifaceted implications. Quantum computing offers promising applications in healthcare, environmental conservation, and artificial intelligence (AI)—extending the boundaries of digital computing beyond current limitations. While quantum and post-quantum cryptography represent more established fields with existing economic players and commercial solutions, the standardization of post-quantum cryptography remains incomplete, albeit with fewer scientific and engineering unknowns compared to scalable quantum computing.

Beyond quantum computing, quantum cryptography has the potential to revolutionize encryption, but it poses implications for state sovereignty—particularly safeguarding sensitive communications. In sensing applications, quantum exists as a real market but is still limited to niche applications. And compared to cryptography and sensing, the maturity of quantum computing is lagging. The feasibility of commercially viable quantum computers remains uncertain, both in the near-term noisy intermediate-scale quantum (NISQ) and the long-term fault-tolerant quantum computing (FTQC) regimes.



Quantum R&D

Quantum technologies continue to be an active R&D and engineering topic for overcoming technological hurdles such as qubit noise, quantum error correction, scalability, and maintaining qubit quality. These uncertainties pose issues that still make for difficult economic and market forecasts. So the possibility of a “quantum winter” remains possible if NISQ systems fail to demonstrate tangible business value. This could potentially slow down investments across the quantum technology ecosystem—affecting public and private funding.

But, at Yole Group, we still believe quantum technologies and specialty computing will lead to an important market value in the medium and long term. In our Quantum Technologies 2024 report, we estimate the total quantum market value will be US$1.832 million in 2029, with US$617 million for sensing.

Quantum computing

Beyond 2030, we expect quantum computing will dominate. In fact, the quantum computing market will

total US$3.736 million in 2035 (both hardware and service). Quantum as a service (QaaS) will hold the major share of this value, with most of the services running on quantum computers in the cloud. It will grow much faster than QC hardware (computers).

Qubits, the fundamental units of quantum computing, come in various forms. The most developed approaches include atoms such as trapped ions (IonQ, Quantinuum, AQT), cold atoms (Pasqal, Infleqtion, Atom Computing) such as rubidium, cesium, and nuclear magnetic resonance (although the latter is less favored for quantum computing; only one company in China sells this type, and it's for educational purposes), superconductors, and photons. Electrons are also used, particularly in nitrogen-vacancy (NV) centers, but with limited industrial players (Quantum Brilliance). Flying qubits, such as photon qubits (and flying electrons), provide alternative approaches to traditional qubits, with vendors such as Psi-Quantum, Quandela, and Xanadu leading in photon qubits.

A quantum computer is based on these different types of physical qubits of a different nature, with each possessing advantages and disadvantages. Most efforts today focus on superconducting qubits, with challengers such as electron spin qubits, NV centers, cold atoms, trapped ions, and photons. No approach is ideal today, and future systems may combine several of them.

Qubits are the technological brick base for quantum computers, which come in different forms. Quantum emulators, used across a spectrum of computing devices from (non-quantum) laptops to supercomputers, execute quantum algorithms via large vector and matrix computations—providing a means to test such algorithms without quantum computers.

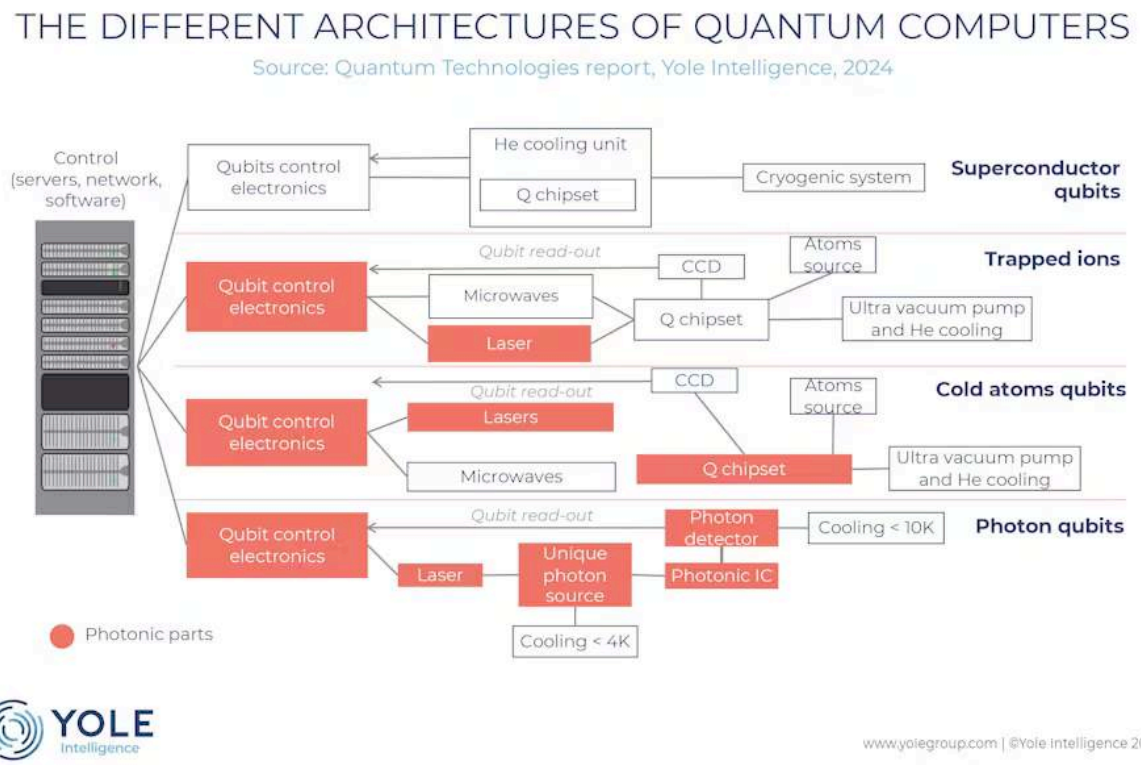
Quantum annealing computers use an adiabatic property, with a set of qubits connected based on specific topologies (like "Pegasus" or "Zephyr" by D-Wave), initialized in the ground state of the Hamiltonian—ensuring convergence toward a low energy state (typically the ground state) and facilitating the search for energy minima to solve various problems such as simulations, optimizations, and machine learning. Meanwhile, digital or universal quantum computers are quantum gates-based. They use qubits equipped with quantum gates capable of executing all quantum algorithms, which makes them general-purpose quantum computers.

But gate-based quantum computers currently have a limited qubit number due to quantum noise. To mitigate this noise, logical qubits made of multiple physical qubits and quantum-error correction codes (QEC) are used. Until fault-tolerant quantum computers with logical qubits become widespread, these systems will rely on non-corrected qubits in NISQ devices. These NISQ computers support 50 to a few-hundred physical qubits and can execute algorithms with limited circuit depth due to qubit error rates.

Efforts are underway to improve their performance using quantum error suppression and mitigation techniques. Eventually, NISQ devices are expected to surpass the computing capabilities of supercomputers for specific tasks. In the future, fault-tolerant quantum computers with many physical qubits and more than 100 logical qubits will revolutionize quantum computing.

Quantum accelerator

At Yole Group, we also see a quantum accelerator on the horizon, functioning as a quantum computer and complementing supercomputers or HPCs by executing variational algorithms where a classical part prepares data for the quantum accelerator and serves as an accelerator within the HPC system and requires close integration for batch loading and executing the quantum algorithm multiple times, typically containing a classical computer within itself.
Whatever the type of qubits and/or the quantum computer architecture, photonics will be of great importance to the development of quantum technologies since lasers and other photonic devices are used for trapped ion/photon/neutral atom technologies. In particular, laser systems are needed for trapped ions, cold atoms, and NV centers. Even if laser suppliers are numerous, only a few can propose systems us-



able for quantum applications. Indeed, agile laser systems with total frequency control, high reliability, and long lifetime are absolutely critical.

To be successful, quantum computers still need to work on size, weight, power, and cost (SWaP-C). Although quantum technologies are long-term, the time to invest is today. Developing a set of toolboxes—such as photonic systems—is a good way to have revenue in the 3- to 5-year term, while also reassuring investors.

3.QuSecure Named as Global Product Leader in Post-Quantum Cryptography Industry by Frost & Sullivan

by Dan Spalding
https://www.businesswire.com/news/home/20240530858272/en/QuSecure-Named-as-Global-Product-Leader-in-Post-Quantum-Cryptography-Industry-by-Frost-Sullivan

QuSecure™, Inc., a leader in post-quantum cryptography (PQC), today announced it has been named as the Global Post-Quantum Cryptography Industry Product Leader by Frost & Sullivan as a result of in-depth research for Frost & Sullivan's "Insights for CISOs: Post-Quantum Cryptography" report.

According to Frost & Sullivan, "PQC constitutes a paradigm shift for the cryptographic systems of the past decades, as well as to how cryptography is used and managed. However, with limited large-scale deployment and implementation to date, organizations need to prepare for potential vulnerabilities and operational complexities that the new algorithms will bring. Enabling full control in an agile and modular way, QuProtect allows organizations to refine their cryptography against such risks and for specific use cases. By offering ease of deployment, adaptability to new requirements, and flexibility of use in individual applications, QuSecure's offering addresses current challenges and future needs."

Frost & Sullivan noted the firm applies a rigorous analytical process to evaluate multiple nominees before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. QuSecure's QuProtect solution was named the industry's product leader over 12 competing solutions based on a thorough evaluation of Product Portfolio Attributes (match to needs, reliability and quality, product/service value, positioning, design); and Business Impact (financial performance, customer acquisition, operational efficiency, growth potential, human capital).

Frost & Sullivan stated, "The idea behind the QuProtect platform echoes the successful approach of moving disparate networking devices to SD-WAN for simplifying and automating operations, improving performance and user experience, increasing agility, reducing costs, and eliminating errors. In a similar way, QuSecure's cryptographic orchestration creates a new layer for cryptographic protocols and algorithms, enabling centralized management, monitoring, and immediate policy changes at scale. Owing to its easy deployment and configurations across devices and applications, QuProtect offers rapid upgrades of legacy infrastructure, interoperability, and policy-driven crypto-agility for current and future regulatory and compliance requirements."

For a copy of the Frost & Sullivan writeup, see: https://www.qusecure.com/qusecure-recognized-as-the-global-post-quantum-cryptography-industry-product-leader-by-frost-sullivan/.

"We are honored to receive Frost & Sullivan's 2024 Product Leadership Award for our QuProtect platform," said Rebecca Krauthamer, Co-Founder and Chief Product Officer at QuSecure. "We built QuProtect to be a true long-term solution for real cybersecurity leaders managing real networks. This recognition further validates that leaders are looking for solutions to usher in this new era of software-defined cryptography, solving encryption upgrade cycles once and for all."

Frost & Sullivan also stated, "Cryptography and crypto-agility will play a much bigger role for organizations in the future. In the context of PQC and beyond, QuSecure brings a disruptive approach to how cryptography is deployed and managed. Coupling full control with simplicity, the company's offering uniquely positions itself in the ecosystem of cryptographic modernization. With the security vendor ecosystem upgrading to PQC in their offerings, QuProtect provides protection for organizations' crown jewels today."

QuSecure's QuProtect software, available now for testing and deployment, offers a comprehensive, end-to-end quantum-security-as-a-service architecture that combines zero-trust, next-generation quantum-resilient technology and crypto-agility to protect networks, cloud systems, edge devices, and satellite communications against today's cyberattacks and future quantum threats, all with minimal disruption to existing systems.

4.FHE, MPC, ZK... The future of Finance

by Bastien Poma

https://www.linkedin.com/pulse/fhe-mpc-zk-future-finance-bastien-poma-d8ftf/?trackingId=lB3-je6wi9qztfoqsFh7zmA%3D%3D

The future of Finance is oriented towards advanced cryptography: FHE, MPC, and ZK. But wait, what do these cryptic acronyms mean? Let's dig together into the technical concepts behind them!

You may have heard the terms of "**Real World Asset**" (RWA) tokenization everywhere by now. RWA stands out as a groundbreaking innovation, by which institutional actors can convert physical and financial assets - bonds, real estate, etc. - into digital tokens on public blockchains. By doing so, they are unlocking liquidity, enhancing transparency, and democratizing access to investments. But the true potential of RWA tokenization is supercharged when combined with cutting-edge cryptographic technologies like Fully Homomorphic Encryption (FHE), Secure Multi-Party Computation (MPC), and Zero-Knowledge Proofs (ZK). But why is that?

Fully Homomorphic Encryption (FHE): FHE allows computations to be performed on encrypted data without decrypting it. This ensures privacy and security in asset tokenization processes, making it possible to handle sensitive financial data while keeping it secure from unauthorized access.

Multi-Party Computation (MPC): MPC enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. In the context of RWA tokenization, this means different stakeholders can collaborate and validate transactions without exposing their private data, thereby enhancing trust and reducing the risk of fraud.

Zero-Knowledge Proofs (ZK): ZK proofs allow one party to prove to another that they know a value without revealing the value itself. This is crucial for ensuring the integrity and authenticity of asset-backed tokens without compromising on confidentiality. ZK proofs can verify ownership and compliance in a seamless and secure manner.

By integrating FHE, MPC, and ZK into the RWA tokenization framework, we can address key challenges such as ensuring privacy, security, and scalability of each transactions on public blockchains, and still guaranteeing auditability and compliance to financial regulations. These technologies not only protect sensitive information but also streamline processes, making asset tokenization more robust and accessible.

Existing bank infrastructures may face significant difficulties in adopting these innovations. Legacy systems often lack the flexibility, scalability, and interoperability required for seamless integration of new technologies. Additionally, compliance and regulatory concerns pose challenges in implementing cryptographic solutions on existing infrastructures. Public blockchains, enhanced by these advanced cryptographic innovations, may appear to be the answer...

5.Concerned about trust in a post-quantum era? You may be more prepared than you think

by Brian Trzupek
https://www.fastcompany.com/91131369/concerned-about-trust-in-a-post-quantum-era-you-may-be-more-prepared-than-you-think

As quantum computing breakthroughs move forward, we've been hearing a steady drumbeat of warnings about their implications. Recent advances in the accuracy and performance of quantum computing are creating serious challenges for maintaining the integrity of digital communications. Experts predict that in less than 10 years, post-quantum computing technology will be capable of cracking today's leading cryptographic security schemes.

IT professionals are closely tracking these developments, and they're expressing concerns. According to a recent Ponemon Institute Report, 61% of IT and IT security practitioners surveyed said they are very worried about not being prepared to address the security implications of post-quantum computing. Yet despite these concerns, the same survey revealed that most lack clarity in ownership, budget, and strategy to prepare for the coming challenges. Only 23% of respondents said they have a strategy for addressing the security implications of quantum computing.

MITIGATING NEW THREATS WITH A PROACTIVE STANCE

As I've spoken with some of our customers, the response to these new developments has been mixed. At a recent informal round table call, participants generally said they were focusing on the most immediate security threats because post-quantum technology is still years away. But we're also hearing that many customers are taking proactive steps to mitigate its impact.

For example, one European organization planning a massive IoT deployment in the coming months is already considering whether their new infrastructure solutions will support post-quantum algorithms and certificates. They have already begun to plan for firmware updates and other preparations before deploying a large volume of devices into the field since these types of updates could prove time-consuming and expensive if they're done after the new equipment is in place.

This organization's approach is a reminder of the need for preparedness and testing, even before new threats arrive. In the Ponemon report, 74% of respondents expressed concern that advanced attackers could conduct "harvest now, decrypt later" attacks, in which they collect and store encrypted data with the goal of decrypting the data in the future.

BUILDING A BALANCED PLAN OF ACTION WITH CRYPTO AGILITY

Post-quantum security threats can impact an entire organization, so a strategic approach based on crypto-agility is key. Crypto-agility combines visibility into where encryption is used and the ability to quickly switch out encryption mechanisms. Strengthening crypto-agility can empower organizations to replace their outdated crypto assets—without a negative impact on their infrastructure and business process.

Implementing a strategy that reaches across the organization may seem daunting, but many organizations have already put some of the core principles of crypto-agility in play.

Digital transformation is already pushing organizations to move at a rapid pace. For example, DevOps teams are constantly testing and iterating as they push the envelope to innovate, get to market faster, and maintain their business advantage. This means organizations may be more ready for post-quantum cryptography than they think—and achieving it is a goal that they can focus on right away.

ADAPTING TODAY'S BEST PRACTICES

What are some practical steps organizations can take to move forward on the crypto-agility journey?

To gain insight into which systems and processes need attention, it's best to start with a thorough inven-

tory. Organizations should not only evaluate processes that are associated with a certificate, but also look well beyond certificates to consider components in their hardware and communications systems such trusted platform modules (TPMs), hardware security modules (HSMs), and secure shell (SSH) connections between servers. DevOps workloads that require code signing might also be vulnerable to post-quantum threats.

An effective inventory will provide a risk-based assessment to help organizations prioritize their protection, enabling them to remediate high-risk areas first as they deploy crypto-agility out into their environment.

Interoperability testing is another key step in getting out in front of the post-quantum threat. Many organizations are already performing extensive testing as part of their development cycles, so this step won't require them to re-invent the wheel, but simply update their existing processes. As they prepare to update cryptographic elements, organizations should test the interoperability of their infrastructure and applications, as well as devices if they are manufacturers.

A close look can reveal unidentified issues and areas that need more attention. For example, when we recently tested a new algorithm for a post-quantum cryptography certificate, we encountered an unexpected timeout in an HSM—which nobody on the team had ever seen before. After some investigation, we learned that the request for the algorithm caused the HSM to enter a safety reset mode, which in turn rippled out across the entire technology stack.

As the NIST prepares to release new post-quantum cryptography algorithms, taking these steps to improve visibility and interoperability will prepare organizations to deploy them with confidence.

THERE HAS NEVER BEEN A BETTER TIME TO EMBRACE CRYPTO-AGILITY

There's no question that the challenge of post-quantum computing is an urgent issue—but it's also one that can be managed with careful planning, good communication, and the right technology partners. Most organizations already understand the value that agility can bring to critical processes and teams like DevOps, and many of the best practices they need are already in place. The time is now to move from business agility to crypto-agility.

6.IDEMIA Secure Transactions Partners with IIT Hyderabad on Post-Quantum Cryptography

https://cxotoday.com/press-release/idemia-secure-transactions-partners-with-iit-hyderabad-on-post-quantum-cryptography/

A leading company in post-quantum cryptography, IDEMIA Secure Transactions has engaged in a research agreement with IIT Hyderabad, one of India's leading technology institutes, to empower future innovators to forge highly secure solutions.

IDEMIA Secure Transactions (IST), a division of IDEMIA Group, today announces a strategic research partnership with Indian Institute of Technology, Hyderabad (IIT Hyderabad) on Post Quantum Cryptography. The objective of the partnership will be to strengthen privacy frameworks against quantum threats,

with a specific focus on designing post-quantum schemes based on lattices and to create post-quantum cryptography solutions that ultimately ensure the long-term security of products. As part of this partnership project, IST will sponsor PhD scholars over a four-year period.

IST's active involvement in advancing post-quantum cryptography efforts in India includes collaborations with key industry and government bodies. The company actively contributes to standardization bodies and organizations in India, including TSDSI, TEC, and CDOT, showcasing its commitment to advancing cryptographic research in the region.

IDEMIA Secure Transactions is committed to fostering innovation globally, having established multiple post-quantum research partnerships with European universities. These collaborations aim to invest in our future and further technological advancements in cryptographic research.

"We are excited to embark on this journey with IDEMIA in advancing post-quantum research. IDEMIA Secure Transactions' unparalleled expertise and commitment to innovation align seamlessly with our vision. Together, we look forward to pioneering ground-breaking solutions that will shape the future of cryptographic systems and safeguard transactions worldwide." said Dr Mudrika Khandelwal, Dean, Alumni and Corporate Relations, at IIT Hyderabad.

"We are very excited to launch this academic partnership with IIT Hyderabad. At IDEMIA Secure Transactions, we are committed to advancing technology and safeguarding information in the post-quantum era. By nurturing the next generation of scholars and engineers and fostering collaborations with esteemed institutions like IIT Hyderabad, we're spearheading the evolution towards a secure digital future." said Paul DISCHAMP, Cryptography & Security Lab Director R&D at IDEMIA Secure Transactions.

7.Terra Quantum Demonstrates QKD Over a 1707 Km (1060 Mile) Fiber Optic Cable

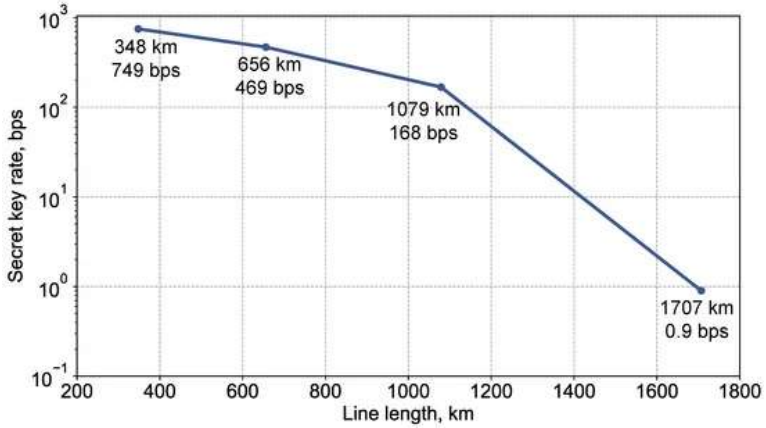
by GQI
https://quantumcomputingreport.com/terra-quantum-demonstrates-qkd-over-a-1707-km-1060-mile-fiber-optic-cable/

One of the current issues with Quantum Key Distribution (QKD) is the limitation of how far a quantum signal can be carried over a lossy fiber optic cable before it becomes unusable. With classical optical networking, this problem is solved using classical repeater technology that measures an incoming optical stream and then regenerates it to send it on to the next link in the chain. However, the approach used in **these classical repeaters won't work with a quantum signal because of the No-cloning theorem**.

Nonetheless, people are testing out QKD networks in what we call metropolitan networks that cover relatively short distances so that repeaters are not needed. Researchers are working on developing quantum repeaters, but at this point no one has a device that is ready to be implemented in a long distance network. Still others are working on technical approaches that can make these metropolitan networks as long as possible without using any repeaters. And **Terra Quantum has just demonstrated one of the longest distances we have seen of 1707 kilometers with their Quantum-Protected Control-Based Key Distribution (QCKD) protocol that utilizes physical control over signal losses**.

Like any optical network, the bit rate will drop with distance. So although they were able transmit a QKD key over a 1707 kilometer line, the bit rate drop dramatically to 0.9 bits per second. To put this another way, at 0.9 bps, **it would take about 284 seconds (or about 4.75 minutes) to transmit a 256 bit key**

that could be used in AES-256. But nonetheless, this is still a considerable achievement.



8.White House Advisor Says NIST to Release Post-Quantum Cryptographic Algorithms in Coming Weeks

by Matt Swayne
https://thequantuminsider.com/2024/05/24/white-house-advisor-says-nist-to-release-post-quantum-cryptographic-algorithms-in-coming-weeks/

The U.S. National Institute of Standards and Technology (NIST) is set to release four post-quantum cryptographic algorithms in the coming weeks, possibly as soon as July, according to a senior White House official, as reported by The Record.

Whenever the release happens, it would mark another important step in the transition to next-generation cryptographic methods designed to withstand the potential threats posed by future quantum computers.

Anne Neuberger, the White House's top cyber advisor, discussed the importance of this release during her address at the Royal United Services Institute (RUSI) in London, The Record reports. She described the release of the algorithms as "a momentous moment," highlighting their role in securing sensitive information against the capabilities of cryptographically relevant quantum computers — CRQCs. These devices, still theoretical, could potentially break current encryption methods, jeopardizing both corporate and national security secrets.

The anticipation of CRQCs has been a growing concern within the cybersecurity community. The Record reports that Conrad Prince, a former GCHQ official and now a distinguished fellow at RUSI, noted that the fear of hostile states decrypting secure messages has been persistent, although the technology has been estimated to be about a decade away for the past 20 years. Neuberger echoed this sentiment, indicating that the U.S. intelligence community expects CRQCs to become operational by the early 2030s.

Action Needed Now

Neuberger also discussed how that prediction isn't an excuse to delay action, due to the "hack now, de-

crypt now" threat.

"The time-frame is relevant because there is national security data that is collected today and even if decrypted eight years from now, can still be damaging," Neuberger explained.

This aligns with warnings from Britain's National Cyber Security Centre (NCSC), which has cautioned that contemporary threat actors could be stockpiling encrypted data with the intent to decrypt it once quantum computers become powerful enough, according to The Report.

"Given the cost of storing vast amounts of old data for decades, such an attack is only likely to be worthwhile for very high-value information," stated the NCSC, as reported by The Record. The looming threat of CRQCs underscores the urgency of developing and implementing quantum-resistant cryptographic solutions.

NIST's upcoming release of these algorithms is a proactive measure to safeguard against future quantum threats. Neuberger highlighted that publishing the new algorithms will help protect the most sensitive kinds of data from being compromised by adversaries in the future.

A NIST spokesperson informed Recorded Future News, "The plan is to release the algorithms this summer. We don't have anything more specific to offer at this time."

Bloomberg is reporting that NIST will specify three PQC-approved encryption algorithms in July.

Just The Beginning

However, the transition to a quantum-resistant computing environment will be more than just the publication of new algorithms. As the NCSC indicates, this step is part of a complex process that includes ensuring current systems can handle the computational demands of post-quantum cryptography.

The underlying security of public key cryptographic systems relies on the mathematical difficulty of factoring large prime numbers, a task that is arduous for classical computers. However, in 1994, American mathematician Peter Shor demonstrated that a quantum computer could efficiently solve this problem, potentially compromising the security of current cryptographic methods.

Despite ongoing advancements in quantum computing, the machines available today are still limited by high error rates, as the NCSC points out. Yet, the possibility of future quantum computers with lower error rates poses a significant threat, making the transition to quantum-resistant cryptography imperative.

9.Post-quantum readiness for TLS at Meta

by Sheran Lin, Jolene Tan, Ajanthan Asogamoorthy, Kyle Nekritz, Rafael Misoczki, Sotirios Delimanolis
https://engineering.fb.com/2024/05/22/security/post-quantum-readiness-tls-pqr-meta/

Today, the internet (like most digital infrastructure in general) relies heavily on the security offered by public-key cryptosystems such as RSA, Diffie-Hellman (DH), and elliptic curve cryptography (ECC). But the advent of quantum computers has raised real questions about the long-term privacy of data exchanged over the internet. In the future, significant advances in quantum computing will make it possible for adversaries to decrypt stored data that was encrypted using today's cryptosystems.

Existing algorithms have reliably secured data for a long time. However, Shor's algorithm can efficiently break these cryptosystems using a sufficiently large quantum computer. Although large quantum com-

puters are not a reality yet, there's an immediate quantum-related threat that needs to be addressed: the "store now, decrypt later" (SNDL) attack, in which attackers intercept and store encrypted data today with the intention of decrypting it at a later date when a sufficiently powerful quantum computer becomes available. This makes transitioning to quantum-resistant cryptography an endeavor of key priority.

To address this issue, the cryptography community has been working on a new class of cryptosystems known as post-quantum cryptography (PQC), which are expected to withstand quantum attacks but can be less efficient (in particular, communication bandwidth wise) than its classical counterparts. The US National Institute of Standards and Technology (NIST) is close to publishing their new PQC Standards (expected to be released this summer). Meta cryptographers are actively contributing to this and other PQC standardization processes (co-authoring the BIKE and Classic McEliece submissions to NIST, and co-editing the ISO/IEC 14888-4 standard).

How Meta is approaching the migration to PQC

Meta's applications are used by billions of people every day. Given our focus on maintaining user privacy and security, Meta continuously raises its security bar to deploy the most advanced security and cryptographic protection techniques. As part of this continuous effort, we've created a workgroup to migrate to PQC, spanning from our internal infrastructure to user-facing apps. This is a highly complex multi-year effort and identifying where to first place PQC protections wasn't trivial.

After careful analysis, protecting components that are susceptible to the SNDL attack, and where we control both endpoints, has been identified as our first priority (given their migration urgency and lack of external dependencies). In particular, protecting our internal communication traffic was the most sensitive use case that checked both boxes and thus became our first migration target.

But a direct migration to PQC wouldn't be the most sensible approach. Migrating systems to different cryptosystems always carries some risks such as interoperability issues and security vulnerabilities. For the PQC migration specifically, the risks are even greater because some of these cryptosystems are comparatively new and/or have not experienced a long period of field testing. To reduce such risks, Meta has started transitioning to using hybrid key exchange for TLS, which combines existing classical cryptographic algorithms with a PQC algorithm. In this way, we ensure that our systems remain protected against existing attacks while also providing protection against future threats.

For our deployment, we have chosen Kyber with X25519 in a hybrid setting. Kyber is the only key encapsulation mechanism selected by NIST for standardization so far. Kyber comes in different parameterizations: Kyber512, Kyber768, and Kyber1024. Larger parameterizations provide stronger security but also require more computational resources and communication bandwidth. We aim to use Kyber768 by default, while using Kyber512 in some cases where larger parameterizations lead to prohibitive performance impact, to accelerate the deployment of PQC hybrid key exchange.

How Meta is enabling PQC

Meta's TLS protocol library, Fizz, is designed for high security, reliability, and performance. The early work on Fizz previously helped standardize TLS 1.3 (RFC 8446). Fizz now supports a range of features including various handshake modes, PSK resumption, Diffie-Hellman key exchange authenticated with a pre-shared key for forward secrecy, async I/O, zero copy encryption, client authentication, and HelloRetryRequest. The use of our own implementation has allowed us to quickly react to new features in the TLS protocol.

Fizz is mostly built on top of three libraries: Folly, OpenSSL, and Sodium. To support PQC, we make use of liboqs, which is an open source library led by world-renowned PQC experts that has received attention from both academia and industry experts. The liboqs library implements post-quantum cryptogra-

phy algorithms for key encapsulation and signature mechanisms, including Kyber. Additionally, we extended Fizz with hybrid key exchange functionality, which can make use of the new post-quantum key exchange mechanisms provided by liboqs alongside existing classical mechanisms.

Challenges

Large packet size

One of the main challenges is the size of the Kyber768 public key share, which is 1184 bytes. This is close to the typical TCP/IPv6 maximum segment size (MSS) of 1440 bytes, but is still fine for a full TLS handshake.

However, the key size becomes an issue during TLS resumption. Internally, we do Ephemeral Diffie-Hellman key exchange to achieve forward secrecy, so key exchange still happens on resumption. There will also be a pre-shared key (PSK) for authentication. These PSKs are 200-300 bytes long, and the remaining ClientHello fields can run up to 200 bytes, causing the resumption ClientHello to exceed the MSS for one packet.

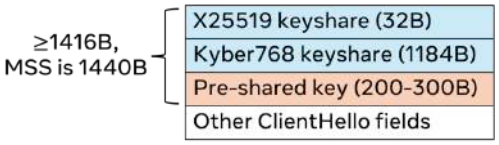


Figure 1: ClientHello size, when including ECDHE keyshares and PSK, will exceed MSS.

This poses some challenges given significant usage of TCP Fast Open (TFO) for internal traffic. With TFO, the entire ClientHello could previously ride along with the TCP SYN packet, allowing the server's TLS implementation to start processing and have its ServerHello ready to send right after its TCP SYN-ACK packet. However, when the ClientHello is too large to fit in the first packet, TFO still happens but the ClientHello is only partially sent. The client then has to wait for the TCP handshake to complete before sending the rest of the ClientHello, and needs to wait again for the ServerHello. This adds an extra round trip time (RTT) to the whole handshake process before any application data can be sent.

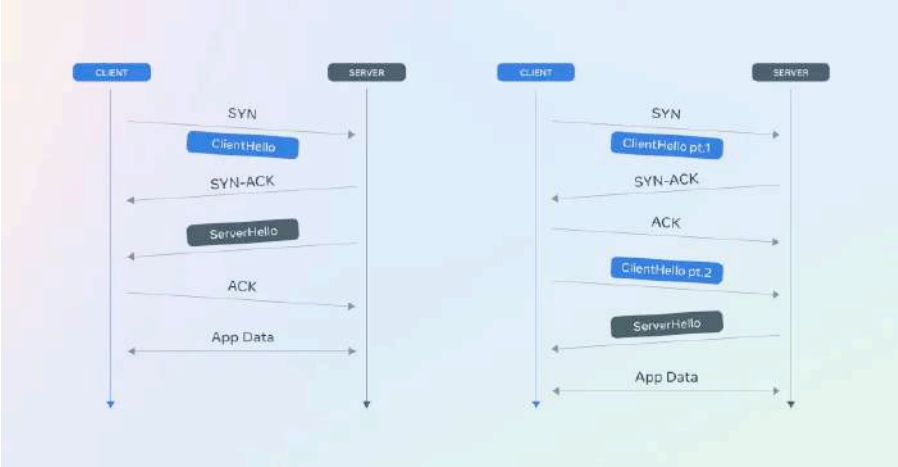


Figure 2: Left: TLS handshake with TFO done in same round trip as TCP handshake.
Right: ClientHello exceeds MSS of one packet, one round trip added to finish TLS handshake.

After evaluating various alternatives and workarounds, and given the prohibitive key size of Kyber768, we opted to use Kyber512 in internal communications affected by this problem for now, allowing us to

accelerate the PQC deployment. Kyber512's 800-bytes-long public keys help with fitting the ClientHello into a single TCP packet, while still being considered secure by NIST. This choice ensures both security and efficient communication. In the future, an increase in MTU, or utilizing QUIC, which allows for multiple initial packets, may allow for larger ClientHellos without an additional round trip.

Multithreading problem with liboqs

After we rolled out post-quantum hybrid key exchange to our fleet, one of our internal teams started experiencing intermittent but constant segmentation fault crashes, and liboqs code was near the top of the stack trace. Here is an example stack trace:

```
#0  0x0000000000000000 in ?? ()
#1  <signal handler called>
#2  0x0000000000000000 in ?? ()
#3  0x0000556ea1ed5eac in keccak_x4_inc_absorb.constprop ()
```

We determined the problem to be a race condition that was causing a function call to call the 0 address. The issue was filed to liboqs. To explain briefly, the race condition was in the Keccak_Dispatch function, where Keccak_Initialize_ptr would be set before setting some other function pointers. Crucially, Keccak_Initialize_ptr being set or not is used by the caller of Keccak_Dispatch to determine whether to actually call it. In a multi-threaded environment, some thread could call Keccak_Dispatch, then set Keccak_Initialize_ptr and pause there. Another thread could then take the same code path, see that Keccak_Initialize_ptr is non-zero and opt not to call Keccak_Dispatch, then call some of the other function pointers that are still zero, leading to a segfault. (The same is true of the Keccak_X4_Dispatch function.)

Although liboqs is being used by a growing number of products and companies, it appears that we were the first to encounter and report this issue, possibly due to the scale of our trial deployment. We fixed it by calling Keccak_Dispatch with pthread_once on POSIX platforms. The fix has since been submitted and merged upstream.

Cross-domain resumption handshake thrash

We rolled out post-quantum hybrid key exchange progressively, with the decision driven by the client. For instance, we started with connections between different data centers, then moved on to traffic within the data center.

Internally, we scope TLS sessions by "service" name. This allows a client to perform cross-host resumption to different servers in the same service. This includes the ability to resume from a server with which the client decides to use hybrid key exchange to one where the client does not, and vice versa, which runs into a small problem with Fizz.

As previously mentioned, we do Ephemeral Diffie-Hellman key exchange on resumption. To facilitate efficient use of computation resources, the client will send only the minimally required default keyshares, which in the resumption case means the keyshare for the previously negotiated named group. This means that when a client connects to a particular server and negotiates a classical named group, then subsequently resumes on a server with which the client should use a hybrid named group, the client would advertise the hybrid named group but send only the keyshare for the classical named group. This leads to the server negotiating the hybrid named group and replying with a HelloRetryRequest to ask the client for the hybrid keyshare, resulting in an additional 1-RTT to perform the key exchange.

To address this, we had the client split each service into different TLS session scopes – one using clas-

sical key exchange, and one using hybrid key exchange. Each session scope thus uses only one named group each, avoiding the keyshare thrashing behavior described above. The tradeoff is space consumption due to having to store more session tickets, but this has been acceptable given the small size of each session ticket (a few hundred bytes).

The computational cost of Kyber key exchange

Meta currently uses X25519 in Elliptic Curve Diffie-Hellman key exchange. During the initial rollout of hybrid key exchange with the hybrid named group X25519_kyber768, we observed a roughly 40 percent increase in CPU cycles. Although this may seem like an undesirable result, it actually indicates that Kyber768 standalone key exchange is faster than x25519, which lines up with results others have found.

Current status and future plans

Meta has deployed post-quantum hybrid key exchange for most internal service communication to protect against the SNDL threat. Since internal service communication traffic occurs within our internal network and is fully under our control, this was the logical starting point for implementing this advanced security countermeasure, even as we await the PQC standards to be published by NIST.

Implementing post-quantum hybrid key exchange to external public internet traffic poses several additional challenges, such as dependency on browsers' TLS implementations and crypto libraries' PQC readiness, increased communication bandwidth due to larger payloads, and more. We are looking forward to industry standardization and major browser based adoption, and we'll keep working across Meta to harden our systems as well. We look forward to sharing more as we continue our efforts in this space.

10.QuSecure Achieves SOC 1 and SOC 2 Type 2 Compliance Validating Security Controls and Practices of its Leading Post-Quantum Cryptography Solution

by Dan Spalding
https://www.businesswire.com/news/home/20240522358771/en/QuSecure-Achieves-SOC-1-and-SOC-2-Type-2-Compliance-Validating-Security-Controls-and-Practices-of-its-Leading-Post-Quantum-Cryptography-Solution-%C2%A0

QuSecure™, Inc., a leader in post-quantum cryptography (PQC), today announced that it has achieved SOC 1 and SOC 2 Type 2 compliance for its QuProtect software solution, validating the rigorous, independent assessment of its internal security controls and practices of its industry-leading PQC solution. This serves as validation of QuSecure's dedication and adherence to the highest standards for security.

"Our successful SOC 1 and SOC 2 reports, completed through an independent third-party assessment, have validated the improvements in our overall security posture," said Craig Debban, CISO at QuSecure. "This attestation is the backbone to creating security products that protect our customers from impending quantum computing and classical threats. This important recognition is also the bedrock to our com-

pliance roadmap which is in direct alignment with growing customer requirements. Maintaining this standard is but one step in our continuing journey to improve our security posture for commercial and government adoption."

Since many organizations require SOC 1 and SOC 2 compliance, such organizations can now be assured that QuSecure has passed rigorous assessments and audits validating the security posture of its post-quantum cryptography and crypto-agility platform, QuProtect. As most organizations require a vendor management review, this new third-party validation immediately attests to QuSecure's ability to meet the toughest security requirements. QuSecure's SOC 3 report is available on request.

QuSecure's QuProtect software, available now for testing and deployment, offers a comprehensive, end-to-end quantum-security-as-a-service architecture that combines zero-trust, next-generation quantum-resilient technology and crypto-agility to protect networks, cloud systems, edge devices, and satellite communications against today's cyberattacks and future quantum threats, all with minimal disruption to existing systems.

11.Zoom bolsters security offering with the inclusion of post-quantum end-to-end encryption in Zoom Workplace

https://news.zoom.us/post-quantum-e2ee/

Today (21 May 2024), Zoom Video Communications, Inc. announced that post-quantum end-to-end encryption (E2EE) is now globally available for Zoom Workplace, specifically Zoom Meetings, with Zoom Phone and Zoom Rooms coming soon. The launch of the new security enhancement makes Zoom the first UCaaS company to offer a post-quantum E2EE solution for video conferencing.

As adversarial threats become more sophisticated, so does the need to safeguard user data. In certain circumstances, attackers may have the ability to capture encrypted network traffic now, with the intent to decrypt it later when quantum computers become more advanced — a scenario often referred to as "harvest now, decrypt later". So, while powerful quantum computers with this capability are not yet generally available, Zoom has taken a proactive stance by upgrading the algorithms designed to be able to withstand these potential future threats.

"Since we launched end-to-end encryption for Zoom Meetings in 2020 and Zoom Phone in 2022, we have seen customers increasingly use the feature, which demonstrates how important it is for us to offer our customers a secure platform that meets their unique needs," said Michael Adams, chief information security officer at Zoom. "With the launch of post-quantum E2EE, we are doubling down on security and providing leading-edge features for users to help protect their data. At Zoom, we continuously adapt as the security threat landscape evolves, with the goal of keeping our users protected."

How post-quantum E2E encryption works

When users enable E2EE for their meetings, Zoom's system is designed to provide only the participants with access to the encryption keys that are used to encrypt the meeting; this is the behavior for both post-quantum E2EE and standard E2EE. Because Zoom's servers do not have the necessary decryption key, encrypted data relayed through Zoom's servers is indecipherable. In addition, to defend against

"harvest now, decrypt later" attacks, **Zoom's post-quantum E2E encryption uses Kyber 768**, an algorithm being standardized by the National Institute of Standards and Technology (NIST) as the Module Lattice-based Key Encapsulation Mechanism, or ML-KEM, in FIPS 203.

Visit our support article to understand which versions and platforms of Zoom Workplace support using post-quantum E2EE.

12.Shall We Regulate Quantum?

by Michael Baczyk
https://quantumcomputingreport.com/shall-we-regulate-quantum-insights-from-the-2nd-annual-stanford-responsible-quantum-technology-conference/

On May 20, 2024, the Stanford Center for Responsible Quantum Technology hosted its 2nd Annual Stanford Responsible Quantum Technology Conference with a focus on Quantum Simulation. The event was a unique blend of art, music, and quantum technology discussions, creating an immersive atmosphere that encouraged open dialogue.

The Stanford Center for Responsible Quantum Technology, founded by Mauritz Kop and part of the Stanford Program in Law, Science & Technology, is an institution dedicated to investigating the societal implications of quantum technologies. The Center brings together a diverse, multidisciplinary community to explore the balance between maximizing benefits and mitigating risks associated with applied quantum technologies, it adopts a pro-innovation stance while navigating the complex landscape of quantum technologies and their ethical, legal, socio-economic, and policy implications (Quantum-ELSPI).

Additionally, the Center has plans to establish a new quantum technology incubator to further support the development of responsible quantum technologies.

During the conference, research fellows from the Center presented their work, which largely built upon the ten principles for responsible quantum innovation proposed by the Center. These principles, organized into three functional categories: safeguarding, engaging, and advancing (SEA), provide a framework for addressing the risks, challenges, and opportunities associated with the development and application of quantum technologies. The principles are linked to central values in responsible research and innovation (RRI) and aim to steer the development and use of quantum technology in a direction that aligns with a values-based society while contributing to addressing society's most pressing needs and goals. Other publications by RQT fellows can be found here.
.
.
.

Regulations of Quantum Technology

The conference also featured discussions on the regulation of quantum technology, with input from various government officials, think tank members, lawyers, and activists based in Washington, D.C. Interestingly, even among the lawyers present, there was a consensus that regulating quantum technology at this early stage might not be the most appropriate course of action. The panelists and speakers noted that it is challenging to predict the full range of applications and implications of any new technology and that regulations often develop in tandem with the field's progress. They suggested that guardrails, recommendations, and best practices are more effective and agile tools for guiding the development of quantum technologies, while standards—an area where the US has traditionally led in many different technologies—are the most ideal. However, it was emphasized that the US should not take its leadership

role in standards in the quantum industry for granted and must actively work to maintain its position.

Given the current technological readiness level of quantum technologies, the speakers argued that regulation might not be the most sensible approach. Attendees from academia, government, and industry alike emphasized the need for international collaboration, stressing that no single country or company can build a quantum ecosystem in isolation. They cautioned that unnecessary or premature regulation could hinder these collaborative efforts. Some speakers even advocated for keeping the future of quantum *as open as possible and only as closed as necessary*, however there were also voices leaning more towards *as closed as possible, open as necessary* approach.

13.NIST Releases First Post-Quantum Cryptography Standards

by Silvia Oakland
https://govciomedia.com/nist-releases-first-post-quantum-cryptography-standards/

The National Institute of Standards and Technology (NIST) said it is looking to transfer all high-priority systems to quantum-resistant cryptography by 2035. Dustin Moody, mathematician in the NIST Computer Security Division, said the transition is necessary for the future because of security concerns with "harvest now, decrypt later."

NIST has standardized three cryptographic algorithms, but post-quantum cryptography will be secure against attacks from classical and quantum computers, officials said. Currently, there isn't a large enough quantum computer that threatens the current level of security, but Moody said that agencies need to be prepared ahead of future attacks.

"Suppose your enemy gets a hold of your data today, and you're not so worried because it's encrypted. But if a quantum computer comes out and say 10 years, and you were hoping that data to be protected for 15 years … you're not going to be protecting your data long enough," Moody said during an ATARC event May 7.

Following a five-year evaluation process, NIST identified in 2022 the four algorithms it would be standardizing and this summer will publish the first post-quantum cryptography standards called Federal Information Processing Standards (FIPS). FIPS will contain three of the four tested algorithms based on code-based cryptography.

NIST selected CRYSTAL-Kyber as the key encapsulation mechanism (KEM) and selected three additional signatures for standardization: CRYSTAL-Dilithium, FALCON and SPINCS+. CRYSTALS-Kyber will be used for general encryption, like securing public-facing websites. CRYSTAS-Dilithium, FALCON and SPHINCS+ will be used when a digital signature is required.

Moody said it's important to begin the quantum transition now, as the process will take some time. NIST, the National Security Agency (NSA), and the Cybersecurity and Infrastructure Security Agency released a joint fact sheet to help agencies navigate cryptographic inventories and discuss the next steps with vendors.

"Make sure your IT people are tracking what's going on with the standardization," he said. "We want you to hold off implementing them in terms of putting them into your products until the final standards come out. But you can certainly test them and see how they will work in your applications," Moody said.

14.Quantum Computing's Impact on Blockchain: Insights from Professor Massimiliano Sala

by Team Ripple
https://ripple.com/insights/Quantum-Computing's-Impact-on-Blockchain-Insights-from-Professor-Massimiliano-Sala/

Each quarter we'll be going under the hood with professors from Ripple's University Blockchain Research Initiative (UBRI) to gain a deeper understanding of trending topics in crypto and blockchain, and highlight their insights and key takeaways. The views expressed in this blog are solely those of Dr. Sala, based on his individual expertise and personal insights.

As part of our ongoing Ripple Insights series, we delve into the rapidly evolving intersection of blockchain and quantum computing with Professor Massimiliano Sala, a renowned Professor of Mathematics at the University of Trento. Professor Sala's expertise in cryptography provides a profound understanding of the quantum challenges facing blockchain technologies, and the XRP Ledger. His work alongside the National Italian Association for the support of study and research in cryptography offers an intriguing vantage point on the broader industry and its development.

Blockchain Security

When addressing what's ahead for the industry, Professor Sala emphasizes the critical vulnerabilities that quantum computing introduces to blockchain security. "Quantum computers could easily solve problems that are foundational to digital signatures, thus potentially undermining the mechanisms that protect users' assets on blockchain platforms," he explains. This vulnerability is particularly concerning for technologies relying heavily on cryptographic security. However, Professor Sala also highlights the proactive strides within the cryptographic community towards developing 'post-quantum' cryptographic schemes that are designed to be secure against quantum computational attacks.

Enhancements in Cryptographic Defenses and Quantum-resistant Algorithms

Looking forward, Professor Sala notes the necessity of transitioning to quantum-resistant cryptographic systems. "All classical public-key cryptosystems should be replaced with counterparts secure against quantum attacks," he states. This transition is crucial for maintaining the integrity and security of blockchain infrastructures against potential quantum threats.

Discussing the development of quantum-resistant algorithms, Professor Sala acknowledges the complexity of integrating these into existing blockchain technologies. He points out the inevitable trade-offs involved, such as increased computational demands and larger data sizes for secure transactions. Despite these challenges, he is optimistic about the ongoing research aimed at optimizing these implementations for practical use.

The Role of Algebra and Coding Theory

Algebra and coding theory play pivotal roles in constructing quantum-resistant cryptographic systems.

Professor Sala illustrates this with examples like the algebraic problem of finding the closest element in a predetermined lattice and the coding-theory-related challenge of decoding noisy data. These mathematical frameworks are crucial for developing robust security solutions that could safeguard blockchain against quantum threats.

Global Collaboration and Quantum Security

Highlighting the importance of international collaboration, Professor Sala praises initiatives like the U.S. NIST standardization process, which has fostered global efforts to establish a common cryptographic standard resistant to quantum attacks. This collaborative approach ensures that new cryptographic schemes undergo rigorous community-wide evaluation, enhancing their reliability and security.

Preparing Future Cryptographers: Blockchain in a Quantum World

From an educational standpoint, Professor Sala stresses the need to revise academic curricula to include quantum-resistant cryptographic methods. This shift requires a transition from traditional cryptographic education, which focuses on integer factorization and discrete logarithms, to emerging challenges that quantum computing introduces.

Professor Sala envisions a future where blockchain technology successfully integrates quantum-resistant cryptographic blocks, thereby mitigating quantum threats. He advocates for a balanced approach to this integration, suggesting that blockchain systems begin by incorporating quantum-safe elements in less critical areas to ensure continued usability.

Quantum Computing Timeline and Practical Steps

Finally, Professor Sala advises organizations to begin transitioning to quantum-resistant technologies immediately. "The probability of quantum threats materializing may not be imminent, but it is significant enough to warrant proactive measures," he asserts. For blockchain developers, he recommends staying engaged with ongoing standardization efforts and participating in forums that focus on quantum-safe advancements.

Through this enlightening discussion with Professor Sala, we gain invaluable insights into the intricate dance of innovation and security at the quantum frontier of blockchain technology. His expertise not only illuminates the path forward but also underscores the critical need for readiness in an era of quantum computing. Professor Sala was recently appointed Head of the Italian Cryptographic Association which includes contributors from universities, banking institutions and research labs among others. You can look forward to hearing more from Professor Sala with plans underway to host a national XRPL Hackathon involving over 20 universities and 60 highly accomplished technical developers on November 21-23, 2024 hosted by the University of Roma Tre.

15.An Introduction to Post-Quantum Cryptography Algorithms

by Christos Kasparis
https://www.eetimes.com/an-introduction-to-post-quantum-cryptography-algorithms/

The rise of quantum computing paints a significant challenge for the cryptography we rely on today. The modern encryption standards we currently use to safeguard sensitive data and communications, such as

DSA, public key RSA and those based on elliptic curves, will eventually be broken by quantum computers. Estimates vary on when, but at current rates of improvement, this is predicted by some to happen towards the end of the next decade.

Michele Mosca, co-founder of the Institute for Quantum Computing at Canada's University of Waterloo, has estimated that there is a 50% chance of a quantum computer powerful enough to break standard public-key encryption materializing in the next 15 years. This means many embedded systems in development now stand a reasonable chance of encountering such an attack by the end of their production run's working lives. It has also been posited that sensitive data can be stored today and decrypted once quantum computers become powerful enough.

This threat extends across various industries, with financial institutions, health organizations and critical infrastructure—including energy and transport—most at risk.

In late 2023, the U.S. National Institute of Standards and Technology (NIST) made a significant step in post-quantum cryptography (PQC), announcing four standardized algorithms specifically designed to resist attacks from quantum computers.

The state of quantum computing

Currently, quantum computers remain in their infancy.

IBM's Osprey is the leading publicly available machine, with 433 quantum bits (qubits), which take on many states at once. In theory, this allows qubits to make calculations much faster. However, advancements are rapid, and experts predict significant increases in qubit count and processing power.

By 2030, quantum computers are expected to surpass traditional computers for specific tasks, with the gap widening further by 2040 and 2050. While not a perfect equivalent to Moore's Law, the exponential growth in quantum computing capabilities necessitates proactive measures to protect cryptographic systems.

The core cryptographic methods

The two most common cryptographic requirements are for public key encryption and digital signatures.

Public key encryption is the mechanism of establishing a shared secret between two parties (e.g. you and your bank), with a public key from your bank and a random number from yourself to enable a secret that you use to encrypt your information.

Until NIST's PQC algorithms, the leading standard was an algorithm based on elliptic curves, which in turn superseded RSA.

Digital signature algorithms are used to authenticate, for example, software releases and prevent message tampering. These use a private key (which is held by the sender) for signing a message, and a public key, which is given to the receiver for authenticating the signed message. Once again, existing algorithms are primarily based on elliptic curves (ECDSA, EdDSA).

The PQC algorithms

Through a collaborative effort, NIST has selected two core (CRYSTALS-Kyber and CRYSTALS-Dilithium) and two backup (FALCON and SPHINCS+) PQC algorithms.

Kyber is a key encapsulation mechanism (KEM) algorithm that uses lattice-based cryptography to enable

small key sizes that are targeted to resource-constrained devices. However, this method generates larger ciphertexts compared to other options.

Kyber is a faster algorithm than elliptic curves and RSA, both in software and hardware. But this also has a larger footprint—be it in terms of software code, or in terms of gates.

Dilithium is a digital signature algorithm designed to supersede DSA. Like Kyber, this uses a lattice-based approach to give highly secure and efficient signing operations for use in high-volume signing needs. Albeit its signature sizes are larger than some competing algorithms.

From early 2023, it was clear that these would be the two core algorithms, and these are the two EnSilica has developed for implementation in ASIC. The additional two algorithms should be seen as supplemental.

FALCON uses a heavier, floating-point arithmetic algorithm for digital signatures. This method means it is slower in comparison to Dilithium, but it does have advantages: it delivers a smaller signature and public key. This makes it more suitable for bandwidth constrained applications.

Like FALCON, SPHINCS+ (Digital Signature is an alternative approach to Dilithium, again using an entirely different mathematical principle—this time a hash-based cryptography—which allows a stateless verification. It has been created in case future weaknesses are found in Dilithium, but has larger signature sizes and is arguably less mature compared to the other algorithms.

It is also important to note that these are just the first steps. More PQC algorithms are under development, and NIST intends to release additional options as the field matures.

Implementations

While PQC algorithms offer solutions, their implementation requires careful consideration. Systems developed today often have lifespans extending beyond the 2030s. As such, adoption has been mandated by national security government bodies—for example, in the U.S., by NSA with the CNSA2.0.

Several major companies are already exploring PQC implementations. At EnSilica, these are focussed on the core two algorithms. Elsewhere, a similar pattern can be seen. Google, for example, pilots Kyber in Chrome; Microsoft integrates both Dilithium and Kyber into its Azure platform; and IBM offers PQC-compatible libraries (its IBM z16 is underpinned by Kyber and Dilithium).

Industry alliances are also forming: The Linux Foundation has announced the launch of the Post-Quantum Cryptography Alliance (PQCA), with founding members including Amazon Web Services (AWS), Cisco, IBM, IntellectEU, NVIDIA, QuSecure, SandboxAQ and the University of Waterloo.

Can you deploy safely in software?

The above shows a mix of hardware and software approaches, but this is often out of necessity. Google, for example, does so because it is unable to control the hardware its web browser is running on.

The standard trade-offs between hardware and software implementations naturally do exist for these algorithms: with hardware both being more resistant to side-channel attacks and delivering enhanced power efficiencies. Indeed, the efficiency advantages of running these algorithms in hardware mean an increased speed of up to 100×.

On the other hand, software implementations enable lower cost systems with the ability to be patched as new algorithms are developed.

There are, therefore, several reasons why you might consider a software implementation. For example, an embedded system that needs to be low cost, with a small area footprint, and where speed is not critical for the application, would be perfectly viable to run the operations in software.

It is also possible to run (and some companies have developed) a hybrid system with both hardware and software components to increase flexibility, albeit with a smaller (10×) increase in speed versus full software models.

We therefore recommend that, for most embedded systems, fully hardware implementations should be the norm.

Forecasted vulnerabilities to address at the design phase

It should also be stated that these algorithms can have weaknesses through their implementation that can be exploited to break them and extract keys.

Examples of these might be timing attacks, where if there are time variations, depending on the exact information the algorithms are processing, this can be exploited to get information out of the algorithm.

Another attack approach might be to measure how much power a chip is consuming and then correlate this to the execution of the algorithm to get information.This means that for both high-security implementations, be it a credit card or SIM cards through to a more general system—for example one holding sensitive data—hardware implementations are essential. Features that act as countermeasures against such attacks need to be developed into the design of any embedded system.

16.The quantum clock is ticking: How quantum safe is your organization?

by Ray Harishankar, Dinesh Nagarajan, Dr. Walid Rjaibi, Gerald Parham, and Veena Pureswaran
https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe?utm_source=substack&utm_medium=email

We can't state it more plainly: the exchange of business value is built upon reliable cryptographic standards. Yet, the everyday *encryption* we take for granted is now under threat—with profound real-world consequences.

First, we need to level-set the misconception that quantum computing is just an esoteric research project. In fact, quantum computing has progressed beyond lab experiments. For example, in June 2023, IBM Quantum and UC Berkeley demonstrated that quantum computers are beginning to outperform leading classical simulations by dramatically improving error mitigation. More recently, IBM demonstrated the ability to improve the efficiency of quantum error correction by nearly a factor of 10.

Increasingly, quantum computing is garnering media attention, with coverage in the *New York Times*, the *Economist,* and the US news show *60 Minutes*.

The possibilities for scientific, medical, and technical breakthroughs are both exciting and astonishing. But the downside of quantum computing's ascendance? Security exposures. Significant ones.

Over the next several years, quantum computing capabilities will jeopardize widespread public-key cryptography (PKC) algorithms such as RSA and Diffie-Hellman. In fact, any classically encrypted communication is already vulnerable to exfiltration. That's because threat actors are already harvesting encrypted communications with the intention of decrypting that data once quantum decryption solutions are available—a technique known as "harvest now, decrypt later" attacks.

The digital economy is dependent on cryptography for establishing and maintaining safe, secure exchanges of value. Once quantum computers become cryptographically relevant, sensitive data—such as financial information, personally identifiable information, phone data, network communications, and intellectual property—could be compromised. The result? Significant financial losses—and worse, a critical loss of trust with customers, partners, and stakeholders. In other words, trust itself is now under threat.

"*Adopting new technologies like generative AI involves balancing enablement with inherent risks. It's important for all organizations to recognize that exposure to quantum threats exists independently of their adoption of quantum computing.*"

—Sujith Surendranathan, Director, Database Security and Data Protection at Sun Life

In short, implementing quantum-safe cryptography is not just sound in terms of security practices. Given our growing dependency on cryptography for the security and safety of our digital world, transitioning to quantum-safe cryptography is essential to preserving the integrity of digital trust mechanisms as a whole.

Recognizing this challenge, the IBM Institute for Business Value (IBM IBV), in partnership with Oxford Economics, surveyed 565 CxOs across 15 countries and 13 industries—all representing organizations with a minimum $250 million in annual revenue. The IBM IBV then analyzed these responses to develop a Quantum-Safe Readiness Index. This index is based on a systematic assessment of organizations' quantum-safe readiness. Assessment outcomes are intended to inform and guide strategic stakeholders about the timeliness and urgency of their quantum-safe transformation efforts.

Overall, organizations in our survey expect that, when starting from their current levels of quantum preparedness, it will take *12 years* to fully integrate quantum-safe standards into their business. In fact, national security guidance requires full compliance with Post-Quantum Cryptography for National Security Systems by 2035. When considering those requirements—along with the lead time needed to identify cryptographic assets and dependencies, implement new standards, and align with partners—the time to begin quantum-safe initiatives is now.

In this report, we explore how Quantum-Safe Champions are driving not only outperformance overall, but a forward-looking mindset that's innately attuned to establishing a quantum-safe culture. We highlight how QSCs cultivate a thriving talent ecosystem. Then, we dive into how, when compared to their counterparts, QSCs report more resilient operations now—and anticipate greater resilience against quantum-enabled security risks. We include steps at the end of each section outlining how organizations can bolster their cybersecurity defenses, as they make plans to implement pending quantum-safe standards. We explain some of the ancillary benefits associated with quantum safety, and how they can position quantum safety as a strategic differentiator.

17.China breakthrough could make 'fault-tolerant' quantum computing a reality

by Zhang Tong

https://www.scmp.com/news/china/science/article/3262459/china-breakthrough-could-make-fault-tolerant-quantum-computing-reality?utm_source=substack&utm_medium=email

Leading quantum physicist Pan Jianwei and his team at the University of Science and Technology of China have **developed an artificial quantum system** that has groundbreaking implications for physics and could pave the way for fault-tolerant quantum computing.

The researchers used photons to simulate an interaction between charged particles known as the fractional anomalous quantum Hall effect, previously observed only in electrons, according to a paper published this month by the journal Science.

Several international experiments have attempted to replicate the Hall effect at the quantum level by putting specific materials through stringent conditions, including strong magnetic fields and extremely low temperatures.

The Chinese researchers developed a new quantum bit – the Plasmonium qubit – to create a clear and flexible artificial system that replicates the phenomenon at normal temperatures without magnetic fields, according to the paper.

The researchers isolated single photons – elementary particles that carry no electrical charge and are also known as quantum light – by boxing them in with a Plasmonium array, making them easier to manipulate and observe.

Chang Jin, vice-president of the Chinese Academy of Sciences (CAS), said the team's achievement in quantum simulation is expected to have a significant impact on the development of quantum technology.

Pan, who is also a CAS academician, said the experiment "demonstrates for the first time that quantum computing can … tackle significant issues in physics. It also significantly advances the development of fault-tolerant quantum computing".

The study's co-author Lu Chaoyang said the team's work "deserves to be included in textbooks". The researchers combined 16 Plasmonium in a 4x4 array, capable of "precisely accommodating a single photon which facilitates observation".

In an interview with CCTV, Lu said the simulated quantum system allows for the construction of equivalent artificial gauge fields without the need for external magnetic fields.

"By precisely controlling the relative energy and connection strength between the boxes, photons within each box are compelled to start 'dancing' with each other, forming a unique pattern as one photon circles around another in two steps," he said.

"One of our major goals is to explore the mysteries of quantum mechanics using entirely new methods. Based on this quantum system, scientists can create some exotic quantum states that do not exist in nature."

Quantum simulation technology will be "an important component of the second quantum revolution", according to state news agency Xinhua.

It is expected to be applied to simulate quantum systems that are … challenging for classical computers, "ultimately achieving quantum computational supremacy", Xinhua said.

Pan and his team are already global leaders in their field, building and launching the world's first quantum satellite Mozi in 2016.

In October last year, they unveiled Jiuzhang 3, a prototype quantum computer which was the first to manipulate 255 photons and can perform specific computations billions of times faster than the world's fastest supercomputers.

While Jiuzhang 3 is not yet applicable to the high computational demands of fields such as cryptography, weather forecasting or material design, a poster visible during the CCTV interview, revealed that its successor is in development.

According to the poster on the lab wall, Jiuzhang 4 – capable of controlling more than 2,000 photons – is expected to be unveiled this year.

18.World-first trial brings scalable quantum security to Europe's largest port, powered by Dutch startup Q*Bird

https://q-bird.nl/2024/05/14/world-first-trial-brings-scalable-quantum-security-to-europes-largest-port-powered-by-dutch-startup-qbird/

Quantum security startup Q*Bird has begun a partnership with the Port of Rotterdam, to upgrade its communications at a time when the security of critical infrastructure is a high priority around the world.

The trial involves Netherlands-based Q*Bird's Falqon® technology being implemented to protect the port's digital infrastructure, as well as its communications with third parties such as customs authorities and logistics service providers that use the port.

Staying ahead of emerging security threats is critical for Europe's largest port.

The port is a key part of the European trade economy. It's the fifth most important bulk port in the world and the 10th largest container port globally. It accommodates 28,000 oceangoing ships and 90,000 inland vessels annually.

The port's communications are already cryptographically secured. But the increasing sophistication of hackers, not to mention the growing geopolitical tensions in the world, make increased security a sensible precaution to protect critical infrastructure such as ports.

Q*Bird provides technology for quantum secure networking. Just as emerging quantum computers or unexpected advancements in classical algorithms could eventually pose a threat to the security of today's strong cryptography, quantum technologies can also provide a solution by offering far stronger security.

"We're using a novel approach by enabling many different users to connect to the same central switch station. This will allow a large number of users to exchange highly secured information," Q*Bird co-founder and CEO, Ingrid Romijn says of the trial.

"This is untappable. And when it is attacked, you will know it."

The trial is a partnership between the Port of Rotterdam Authority, Q*Bird, Portbase, Single Quantum,

Cisco, Eurofiber, Intermax and InnovationQuarter. At MWC24 in February, Q*Bird and Eurofiber, a provider of industry-leading open digital infrastructure, announced a partnership to offer the highest standard of network security thanks to quantum technology.

19.Awareness about Quantum Threat is There. Now It's Time to Take Action – Lessons from RSA Conference

by Michael Baczyk
https://quantumcomputingreport.com/awareness-about-quantum-threat-is-there-now-its-time-to-take-action-lessons-from-rsa-conference/

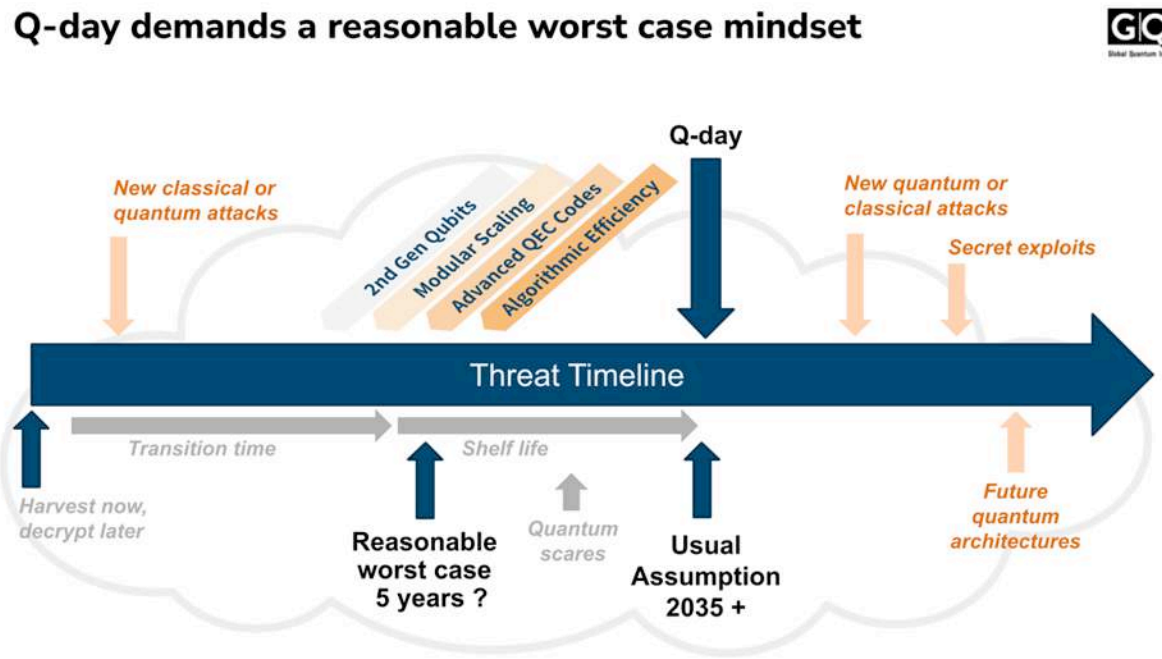
Is Quantum on the Agenda of Security Executives?

The RSA Conference, the world's premier cybersecurity event, convened in the heart of San Francisco, attracting over 40,000 attendees from around the world. The sprawling exhibition hall showcased the conference's immense scale, requiring a full day to thoroughly explore each booth. For more than three decades, the RSA Conference has been a driving force behind the cybersecurity community, expanding its mission beyond annual gatherings to provide continuous support in the face of ever-evolving cyber threats. One of the most pressing concerns is the looming quantum threat, and my primary objective was to gauge the level of awareness and action among governments and commercial players in preparation for Q-day. The conference flew by in a flurry of intense discussions and networking, with days packed with hundreds of conversations. RSAC caters to decision-makers in the field, with 44% of attendees holding positions at the Director, VP, or C-level. I was pleased to discover that awareness of the quantum threat was widespread, with nearly everyone having seen news, heard discussions, or engaged in conversations about quantum computing. However, this awareness did not necessarily translate into immediate, well-defined actions or concrete plans for most of the attendees. While each organization's roadmap will differ based on its size and agility in adopting new solutions, it is universally clear that the transition to post-quantum cryptography (PQC) should be one of the priorities on every company's agenda.

There were also encouraging signs that concrete actions are beginning to enter the collective mindset. Many booths not belonging to quantum vendors prominently featured "Post-Quantum Cryptography" as part of their product offerings. Moreover, I heard accounts of companies proactively reaching out to large security firms to initiate the transition to the post-quantum security era. These instances were not limited to banks or financial institutions; I also heard specific examples from the retail sector. While post-quantum cryptography (PQC) is essential for mitigating the risks posed by quantum computers, it represents only one facet of the quantum realm. Preparing for the quantum threat is crucial, but it is equally important to recognize that quantum technologies can also bolster cybersecurity.
The latest topics discussed at RSAC in the post-quantum cryptography (PQC) area included:

1. **PQC Standardization:** The ongoing PQC standardization process led by the National Institute of Standards and Technology (NIST) has been a focal point of discussion, especially with the anticipation of initial PQC standards being released in 2024. The cybersecurity community is eagerly awaiting NIST's next moves and the implications for the industry.

2. **Hardware Efficiency Challenges:** One significant concern raised was the hardware inefficiency of



some proposed PQC schemes. Certain protocols are resource-intensive, making them challenging to implement in a wide range of applications. Addressing these hardware constraints is crucial for the practical adoption of PQC solutions.

3. **PQC Adoption Strategies:** Startups in the PQC domain are grappling with the question of how to effectively sell their solutions. One approach gaining traction is penetrating the supply chain by licensing PQC technologies to established security vendors. This strategy enables PQC startups to leverage the existing customer base and distribution channels of these vendors, facilitating a smoother transition to PQC for end-users.

4. **Legacy System Compatibility:** Many organizations still rely on legacy systems, such as older versions of Microsoft Windows, which may not receive PQC support from the original vendor. This presents a challenge for ensuring comprehensive quantum resilience. PQC startups are exploring ways to offer intermediate layers or adaptors to bridge the gap and provide quantum-resistant security for legacy systems.

5. **Export Control of PQC Solutions:** Some PQC companies may face export control restrictions, limiting their ability to sell their solutions to countries outside of NATO. This adds a layer of complexity to the global adoption of PQC technologies, as companies navigate the legal and regulatory landscape to ensure compliance with export control regulations while still striving to promote widespread implementation of quantum-resistant security measures.

6. **Growing Interest in the Automotive Industry:** With the rapid digitalization of vehicles and the trend towards autonomous driving, the automotive industry is showing increased interest in PQC. Securing in-vehicle systems, communication networks, and infrastructure against quantum threats is becoming a priority for automotive manufacturers and suppliers.

The PQC landscape at RSAC 2024 featured a diverse range of players, each bringing their unique expertise and offerings to the forefront. Notable vendors present included established names such as QuSecure, SandboxAQ, PQShield, Quantropi, and Quintessence Labs, as well as relatively new entrants like pQCee and Quantum Knight.

It is essential to recognize that while these vendors collectively operate within the PQC domain, their specific focus and approach may vary significantly. Some players concentrate exclusively on software-based solutions, developing algorithms, libraries, and toolkits to enable the integration of PQC into existing systems. Others take a more holistic approach, combining software development with hardware innovations to provide comprehensive PQC solutions.

The scope of offerings also differs among vendors. Some companies provide full-suite cybersecurity solutions that encompass various aspects of quantum-resistant security, including key management, authentication, and secure communication protocols. Others choose to specialize in specific areas, such as the encryption layer, focusing on the development and implementation of quantum-resistant cryptographic algorithms. Furthermore, while all these vendors are united in their efforts to address the quantum threat through PQC, some extend their operations to complementary technologies that harness the power of quantum mechanics to enhance security.

In recent years, the cybersecurity landscape has been dominated by software-based solutions, with a strong emphasis on developing and deploying advanced algorithms, protocols, and frameworks to combat evolving threats. Not to mention AI that was a hot topic of this year's RSAC as well.

In order to provide the highest quality when generating cryptography keys, Quantum Random Number Generators (QRNG) are available in both software and hardware implementations, catering to the diverse needs of the industry. Notable players in the QRNG space include Quantinuum, which offers a software-based deployment solution, and Qrypt, which has recently started showcasing its hardware-based QRNG solution at conferences. Other companies present at RSAC, such as Quantropi and Quintessence Labs, have integrated QRNG capabilities into their broader security suites, recognizing the critical role of high-quality entropy in cybersecurity.

Quantum key distribution (QKD) is also gaining traction, particularly in Europe and Asia, not so much in the US. QKD allows for the secure exchange of cryptographic keys over untrusted networks, leveraging the principles of quantum mechanics to detect any attempts at interception or manipulation. Quintessence Labs present at RSAC has shipped its continuous variable quantum key distribution (CV-QKD) hardware out of Australia, demonstrating the growing demand for QKD solutions in the global market.

All in all, it was a very busy RSA Conference. Although there are a large number of cybersecurity threats that IT professionals need to be concerned with, it is encouraging that there is increased understanding of how a quantum-based attack can affect an organization's security. Certainly, now is the time to start planning on how your organization will implement the necessary precautionary measures. One needs to understand that these measures will take a long time to fully implement, and it will be very costly for those who wait too long.

20.NVIDIA Accelerates Quantum Computing Centers Worldwide With CUDA-Q Platform

by NVIDIA
https://nvidianews.nvidia.com/news/nvidia-accelerates-quantum-computing-centers-worldwide-with-cuda-q-platform?utm_source=substack&utm_medium=email

NVIDIA today announced that it will accelerate quantum computing efforts at national supercomputing centers around the world with the open-source NVIDIA CUDA-Q™ platform.

Supercomputing sites in Germany, Japan and Poland will use the platform to power the quantum processing units (QPUs) inside their NVIDIA-accelerated high-performance computing systems.

QPUs are the brains of quantum computers that use the behavior of particles like electrons or photons to calculate differently than traditional processors, with the potential to make certain types of calculations faster.

Germany's Jülich Supercomputing Centre (JSC) at Forschungszentrum Jülich is installing a QPU built by IQM Quantum Computers as a complement to its JUPITER supercomputer, supercharged by the NVIDIA GH200 Grace Hopper™ Superchip.

The ABCI-Q supercomputer, located at the National Institute of Advanced Industrial Science and Technology (AIST) in Japan, is designed to advance the nation's quantum computing initiative. Powered by the NVIDIA Hopper™ architecture, the system will add a QPU from QuEra.

Poland's Poznan Supercomputing and Networking Center (PSNC) has recently installed two photonic QPUs, built by ORCA Computing, connected to a new supercomputer partition accelerated by NVIDIA Hopper.

"Useful quantum computing will be enabled by the tight integration of quantum with GPU supercomputing," said Tim Costa, director of quantum and HPC at NVIDIA. "NVIDIA's quantum computing platform equips pioneers such as AIST, JSC and PSNC to push the boundaries of scientific discovery and advance the state of the art in quantum-integrated supercomputing."

The QPU integrated with ABCI-Q will enable researchers at AIST to investigate quantum applications in AI, energy and biology, utilizing Rubidium atoms controlled by laser light as qubits to perform calculations. These are the same type of atoms used in precision atomic clocks. Each atom is identical, providing a promising method of achieving a large-scale, high-fidelity quantum processor.

"Japan's researchers will make progress toward practical quantum computing applications with the ABCI-Q quantum-classical accelerated supercomputer," said Masahiro Horibe, deputy director of G-QuAT/AIST. "NVIDIA is helping these pioneers push the boundaries of quantum computing research."

PSNC's QPUs will enable researchers to explore biology, chemistry and machine learning with two PT-1 quantum photonics systems. The systems use single photons, or packets of light, at telecom frequencies as qubits. This allows for a distributed, scalable and modular quantum architecture using standard, off-the-shelf telecom components.

"Our collaboration with ORCA and NVIDIA has allowed us to create a unique environment and build a new quantum-classical hybrid system at PSNC," said Krzysztof Kurowski, CTO and deputy director of PSNC. "The open, easy integration and programming of multiple QPUs and GPUs efficiently managed by user-centric services is critical for developers and users. This close collaboration paves the way for a new generation of quantum-accelerated supercomputers for many innovative application areas, not tomorrow, but today."

The QPU integrated with JUPITER will enable JSC researchers to develop quantum applications for chemical simulations and optimization problems as well as demonstrate how classical supercomputers can be accelerated by quantum computers. It is built with superconducting qubits, or electronic resonant circuits, that can be manufactured to behave as artificial atoms at low temperatures.

"Quantum computing is being brought closer by hybrid quantum-classical accelerated supercomputing," said Kristel Michielsen, head of the quantum information processing group at JSC. "Through our ongoing collaboration with NVIDIA, JSC's researchers will advance the fields of quantum computing as well as chemistry and material science."

By tightly integrating quantum computers with supercomputers, CUDA-Q also enables quantum computing with AI to solve problems such as noisy qubits and develop efficient algorithms.

CUDA-Q is an open-source and QPU-agnostic quantum-classical accelerated supercomputing platform. It is used by the majority of the companies deploying QPUs and delivers best-in-class performance.

21.Why Quantum Breakthroughs May Turn Industry Titans Into Dinosaurs

by Tom Dakich
https://www.spiceworks.com/tech/networking/guest-article/quantum-communication-revolution/

Tom Dakich, CEO of Quantum Corridor, says quantum communication networks promise lightning-fast data transmission and unmatched security, revolutionizing telecom. But are we ready for this quantum leap?

Real-world applications for quantum technology are moving ever closer, but the breakthroughs that will put quantum research on a fast track to commercialization are found in quantum communication (QComm) networks. By pairing near-instantaneous transmission with massive throughput, QComm will offer extraordinary opportunities and challenges that will permanently disrupt the telecommunications industry.

Chip manufacturers already produce advanced graphics processing units (GPUs) that perform the parallel calculations needed for artificial intelligence and high-performance computing. Quantum computing advances may be only a year away from bringing us quantum processing units (QPUs), which use the behavior of particles like photons or electrons to make calculations. QPUs calculate in qubits, which can represent many different quantum states, and so can solve certain problems extraordinarily faster than traditional chips, which use on/off states of electrical current that represent zeros or ones.

To link these quantum-based platforms efficiently, QComm networks will be required. Yet the vast, decades-old optical fiber infrastructure of modern telecommunications did not anticipate this need.

To take advantage of the coming speed breakthroughs, telecoms will need to partner with and invest in the innovators pushing quantum commercialization. Quantum-based networks will power extraordinary innovations across many fields, from chemistry and biology to materials science, AI, and machine learning.

Quantum Positioned to Resolve Speed, Security Barriers

By employing quantum states of light, QComm is emerging as the answer to two needs: speed and security.

When distributed compute clusters are upgraded to quantum compute clusters, as expected, QComm

will be essential. In this environment, real-time transfer of vast amounts of information will be required. While research facilities and data centers have used quantum computers for 25 years, most computing and transmissions occur in individual labs unconnected to other labs. Quantum-speed networks will make those connections possible.

Solutions exist to ramp up the speed and capacity of today's infrastructure, but not without investment in new technology. For example, coherent optical switches can transmit the entangled photons of a quantum network. Quantum Corridor has employed a coherent fiber-optic network to transmit classical data from Chicago to Hammond, Indiana, at 40 terabits per second (Tbps), or 40,000 times faster than the gigabit internet. By the end of the year, this coherent fiber-optic network will scale to a quantum-ready 1.2 petabits per second (Pbps)— equal to 600 billion pages of text transmitted every second, or nearly the entire data exchange of the internet backbone today (1.7 Pbps).

Coherent optics will provide existing fiber infrastructure, such as the State of Indiana's 172-mile-long line of fiber-optic cable and the speed and capacity that quantum computing will need. Yet quantum data is prone to degrade over long distances. Developing long-distance networks will require an architecture to ensure that such communication is lossless. Space exploration ventures, AI entrepreneurs, and e-commerce hyperscalers will need this network to support their work.

Even before quantum computing clusters see wide adoption, existing applications may require more telecom capacity. Today, a Google search touches some 4,000 servers. Add complex AI modeling invoking machine learning algorithms, then add 4K video streaming and 8K virtual reality applications offered by the likes of Meta's Oculus headset. These bandwidth requirements will strain the capacity of existing networks.

Higher telecom capacity also will enable enhanced encryption techniques to keep communications secure. Once quantum computers break classical protocols like SSL and TSL, advanced encryption techniques will be vital to spur research and commercialization in economic sectors, from financial services to pharmaceutical research to national defense. This vulnerability is not just theoretical. GPU miners already solve blockchain algorithms today, albeit slowly —a single, top-of-the-line GPU would need 1,000 years or more to solve one Bitcoin. QPU processors will radically change this calculation.

Information security is also advancing rapidly in both enterprise software and commercial applications, such as Apple's Post Quantum Encryption (PQE) for the iMessage app. Classical techniques from the BB84 protocol to post-quantum cryptography algorithms will be supplemented by cryptographic techniques that involve quantum superposition. Whatever the method, telecom networks will need to support a higher level of security.

Managed Networks Light the Path to a Quantum Internet

How will QComm networks emerge? In my view, given the pace of quantum breakthroughs and the exceptional amounts of experimentation, testing, and adaptation needed, they will arrive as purpose-built deployments, connecting the likes of defense contractors and facilities, major industrial researchers or biotechnology labs. As these next-generation networks arrive, they will link with QComm research sites, such as the Chicago area fiber network at Argonne National Laboratory.

And there are plenty of challenges left that will require major investment. A 2023 McKinsey analysis tallied the 2022 investment in quantum technology start-ups, including companies in quantum computing, communications, and sensing, at $2.35 billion. Investments fall into three categories:

- Components, ranging from lasers, detectors, cryostats, specialized fibers and other technologies.
- Hardware, including functional quantum repeaters to extend the range of these networks.

- Software, for applications and services.

To enable the flow of valuable and sensitive data, each type of investment must be American-made to comply with the Trade Agreements Act (TAA). Federal contracts will mandate edge security for devices that connect to the network. A future of more precise quantum sensors will put further demands on security, extending to the network's components.

Through no fault of their own, in the last two decades and nearly half-trillion dollars spent migrating from copper to fiber optics. It is no criticism to see conventional providers are not structured to lead the quantum commercialization effort. Public policy will set performance standards and limit the risk of infiltration. This framework will take much work to achieve on distributed networks with many access points. Inevitably, separate quantum communication services will emerge.

The challenge for any quantum communication service provider will be to nurture today's early-stage quantum technologies. The competition will not be about speed or bandwidth but about supporting commercial applications that could solve society's most vexing problems.

Innovators that create a fertile ground for advanced communication between the smartest computers and the smartest people in the world will succeed. Telecoms, hyperscalers, and others will unquestionably benefit from this activity. The telecom titans will be welcomed as colleagues, investors, and partners who will help scale QComm into the future.

22.EU Commission publishes recommendation on Post-Quantum Cryptography implementation

by IDQ
https://www.idquantique.com/eu-commission-publishes-recommendation-on-post-quantum-cryptography-implementation/?utm_term=EU%20Commission%20publishes%20Recommendation%20on%20Post-Quantum%20Cryptography%20implementation&utm_campaign=Quantum%20Era%20Security%20Times%3A%20May%202024&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%3A%20May%202024-_-EU%20Commission%20publishes%20Recommendation%20on%20Post-Quantum%20Cryptography%20implementation

The European commission has issued a paper urging on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. It encourages Member States to develop and implement a harmonised approach as the EU transitions to post-quantum cryptography. This aims to ensure that the EU's digital infrastructures and services are secure in the next digital era.

As part of it, the EU Commission encourages hybrid schemes that combine Post-Quantum Cryptography (PQC) with existing cryptographic approaches or with Quantum Key Distribution (QKD).

That's good news. The migration to quantum-safe communication can be significantly derisked and ac-

celerated with the appropriate use of cryptographic hybridization: the deployment of QKD in the existing telecommunication backbone infrastructure can be combined with PQC thanks to IDQ's new Quantum Key Exchange platform: Clarion KX.

This defence in depth approach mitigates the long-term risk to the data posed by the rapidly emerging quantum threat and it guarantees end-to-end security on any location in the network. Furthermore, a sound combination of QKD and PQC allows for increased cryptographic agility, while minimizing the ongoing investment in time and resources.

23.Terra Quantum Launches TQ42 Cryptography Library for Secure Data Transmission, Storage and Authentication

by Terra Quantum
https://www.hpcwire.com/off-the-wire/terra-quantum-launches-tq42-cryptography-library-for-secure-data-transmission-storage-and-authentication/

Terra Quantum, a leader in quantum technology solutions, today announced the launch of TQ42 Cryptography, an open-source post-quantum cryptography library. This cutting-edge suite of quantum-resistant algorithms is designed to help businesses protect their data from current and future security threats. The expansion of its TQ42 quantum-as-a-service ecosystem complements TQ42's existing offerings that provide easy access to quantum computing tools.

Future quantum computers pose a significant threat to the digital world. Experts estimate that a quantum computer with just a few thousand logical qubits could break widely used encryption schemes, putting sensitive data at risk.

Terra Quantum's patented Quantum Key Distribution (QKD) protocols published in Nature's Scientific Reports set the world record for securing long-distance communications with quantum encryption in 2023 and offer security for data in motion. To secure data at rest, strong algorithms such as those provided in the TQ42 Cryptography library are required.

``The addition of TQ42 Cryptography to the TQ42 ecosystem is a significant step, enabling organizations to start their journey towards quantum-securing their data," said Markus Pflitsch, CEO of Terra Quantum. "It complements our existing QKD solution, providing a holistic approach to quantum security for both data in motion and data at rest."

TQ42 Cryptography provides developers with a comprehensive suite of post-quantum algorithms, security and key management functions, including:

- Classic Quantum-Resistant Algorithms with Hash Functions and Symmetric Encryption.
- Asymmetric Post-Quantum Algorithms.
- Key Management with Secure File Deletion, Pseudo Random Key Generation, and an Encrypted Saving to File System.

Encompassing a wide range of applications, TQ42 Cryptography can be implemented across diverse platforms such as mobile, web applications, IoT, cloud and others. Some example of use cases include:

securing smart home automation systems, enhancing Wi-Fi and Blockchain security, and achieving Perfect Forward Secrecy in sharing information.

``As organizations begin to plan for the post-quantum future, adopting appropriate cryptography solutions is crucial for maintaining the security of valuable information," said Dr. Florian Neukart, Chief Product Officer of Terra Quantum. "TQ42 Cryptography provides an accessible entry point to start integrating quantum-resistant security measures into their applications, ensuring the long-term protection of sensitive data."

TQ42 Cryptography caters to the needs of developers and security professionals by offering a user-friendly API, scalable architecture, and essential security features like key generation and file deletion capabilities. The library is available under two primary licensing options to accommodate the needs of organizations at different stages of their post-quantum migration journeys: Free Use is permitted under AGPLv3 and a Commercial licence is also available. Contributions will be welcomed in the near future under a Contributor license.

Later this year, Terra Quantum will expand the library to include support for Python, iOS and Android, additional post-quantum algorithms, and upgrade options, like the ability to purchase quantum keys generated from Terra Quantum's proprietary Single Photon Quantum Random Number Generator (QRNG), which is designed and implemented according to the latest NIST standard (SP 800-90B) and certified by METAS.

The company also intends to expand the TQ42 ecosystem with the introduction later this year of Entropy-as-a-Service. This product will leverage their proprietary Quantum Random Number Generator (QRNG) to provide organizations with access to true random numbers, a critical component in secure cryptographic operations.

Additionally, the upcoming Quantum Keys-as-a-Service offering will utilize Terra Quantum's proprietary Key Containers with encryption, enabling organizations to securely manage and distribute cryptographic keys. These advanced offerings will provide organizations with the opportunity to upgrade to the highest level of security and true entropy from quantum keys, building upon the foundation laid by TQ42 Cryptography.

24.Study of Quantum Computing Use Cases Developed Worldwide

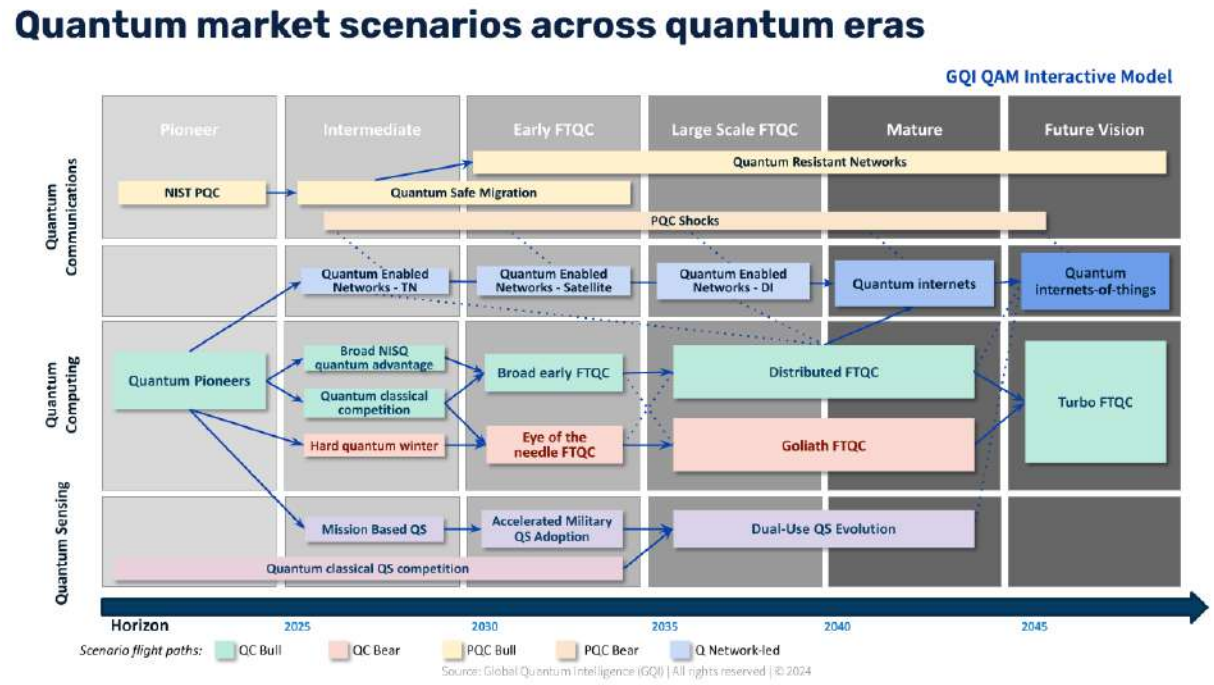
by Michael Baczyk
https://quantumcomputingreport.com/realizing-quantum-potential-study-of-quantum-computing-use-cases-developed-worldwide/

Quantum Computing is a high-stakes game

The recent news of PsiQuantum securing one billion Australian dollars in funding from both the Australian federal and regional governments has caused quite a stir in the tech world, sparking excitement and even controversy. This development has compelled even the most skeptical observers to acknowledge that quantum technology is poised to become the next major advancement in the tech industry. The PsiQuantum deal is just one example of the intensifying efforts from both commercial and national strategic perspectives. Quantum technology is already recognized as a significant value enabler and has secured a prominent position on key national agendas, particularly in the realm of cybersecurity.

According to the Global Quantum Intelligence QAM (Quantum Addressable Market) Engine, while the current Total Addressable Market (TAM) for Quantum Computing is still limited, projections for 2030 indicate that the market may approach 10 billion dollars and above 25 billion dollars in 2035. These predictions are based on a comprehensive study of quantum computing use cases and how their value will be realized by specific players in the value chain, considering all plausible scenarios that may unfold in the quantum landscape. Consequently, this figure represents the current best estimate, contingent upon the trajectory that quantum technology follows.

In the coming years (2025-2030), we anticipate three potential scenarios in the Quantum Computing realm. The first and most optimistic scenario involves the realization of Broad Quantum Advantage, primarily due to advancements in error handling efforts. The second scenario entails the continuation of the current Quantum vs. Classical competition, characterized by claims of supremacy being issued and potentially subsequently debunked by other players in the field or enthusiasts. The third and more pessimistic scenario is the possibility of a Hard Quantum Winter.



Nonetheless, as we continue to look ahead (recognizing that quantum is a domain for the patient and strategic thinkers), the end of the decade emerges as a critical intersection for many currently published roadmaps. We have previously reported and analyzed these roadmaps from industry leaders such as IBM, Microsoft, Pasqal, and QuEra.

Methodology of the overview

At Global Quantum Intelligence, we diligently track organizations involved in quantum technology worldwide. Our team analyzes the commercial progress of quantum computer vendors, large enterprises, quantum consortium initiatives, and academic breakthroughs achieved by universities, as well as private and government R&D institutes. For this study, we conducted a thorough examination of press releases, partnership announcements, and a vast array of scientific publications in peer-reviewed journals and those released on arXiv. By leveraging our extensive GQI database, we curated a truly global collection of organizations developing quantum computing use cases.

To ensure the integrity and relevance of our findings, we applied stringent criteria when classifying examples as use cases in this study. Each use case must demonstrate commercial relevance, provide hardware requirements, solve a specific problem, and detail the limitations of the approach. We intentionally exclude progress in algorithms or quantum subroutines, even in hybrid settings, as we consider these to be of more academic relevance. Our clients are primarily interested in the current state of the market, and that is precisely what we deliver.

The accompanying map illustrates the distribution of the 268 organizations we have categorized as quantum computing use case developers. While the United States carries the most weight on the graph, correlating with its leading position in terms of the number of quantum computing startups worldwide, Europe as a whole carries an equivalent weight. China and Japan are also well-represented, and the majority of the globe is covered, albeit in smaller proportions. This global representation is a clear indication that awareness of quantum computing is spreading across the world with 36 countries being represented.

What industries are already looking into quantum computing?

Our analysis encompasses 172 use cases across 8 industries: Security & Defence, Life Sciences, Infrastructure, Health, Financial Services, Energy & Resources, Chemicals & Materials, and Advanced Industries. We have also included a 9th group, Multiple Industries, for use cases with a broader scope and applicability range. Within each of these groups, we further segmented the use cases based on their implementation status.

The top three industries in terms of the number of use cases being developed are Advanced Industries, Financial Services, and Life Sciences, each boasting over 50 use cases. Chemicals & Materials and Energy & Resources closely follow the leading industries, with more than 30 use cases each. Infrastructure, Health, and Security & Defence have fewer than 10 use cases currently in development.

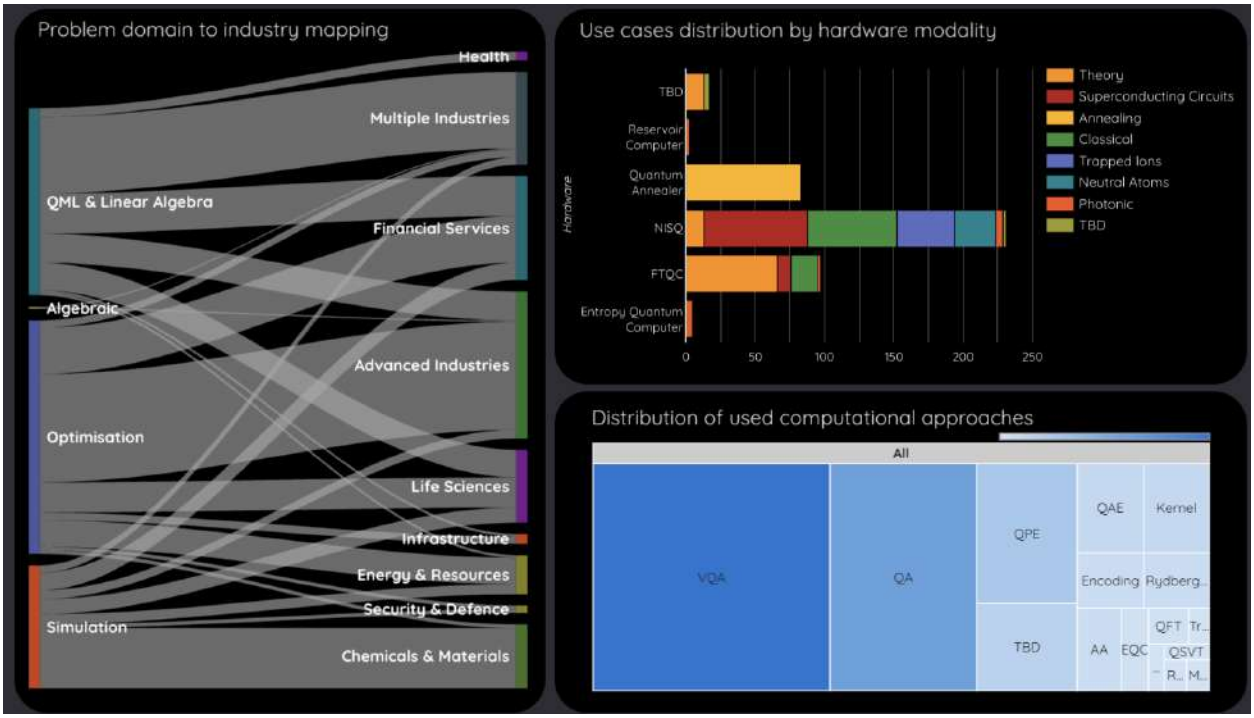
When examining the implementation status of these use cases, we observe that a significant percentage are toy demonstrations, accompanied by classical simulations, problem formulations, theoretical considerations, and speculations. This suggests that while there is substantial interest and effort being invested in quantum computing applications across various industries, many of these use cases are still in

the early stages of development and have yet to be fully realized in practice. There are only a few cases marked as In Deployment.

Technological overview of Quantum Computing use cases

Within each of the industries introduced in the previous paragraphs, we are particularly interested in the problem domains that researchers and developers are attempting to solve using quantum computing. We have identified four distinct problem domains: **QML & Linear Algebra, Algebraic, Optimization, and Simulation**. The left side of the figure illustrates the mapping of these problem domains to their respective industries. Optimization emerges as the largest group, with significant importance in Advanced Industries, Financial Services, and Energy & Resources. While QML & Linear Algebra applications also have a strong focus on finance, they tend to be more industry-agnostic, targeting Multiple Industries simultaneously. Simulation is the problem domain most frequently encountered in Chemicals & Materials and Life Sciences.

The right-hand side of the figure reveals that the majority of use cases aim to extract commercial value from quantum computing as quickly as possible. NISQy hardware and Quantum Annealers are the most widely used, and in terms of computational approaches, variational algorithms and quantum annealing algorithms account for more than half of the techniques employed.



On the other hand, the theory for fault-tolerant quantum computing (FTQC) appears to be well-established, with some initial, highly promising commercial ideas and the underlying algorithms, such as Quantum Phase Estimation and Quantum Amplitude Estimation, offering theoretical guarantees.

This suggests that while near-term applications are currently the primary focus, there is a strong foundation being laid for the future of quantum computing, with FTQC approaches poised to deliver significant value once the hardware matures.

The inflection point for the industry is yet to come

Since 2015, Quantum Computing Report has been at the forefront of reporting on the latest advancements in quantum technology. The accompanying plot clearly illustrates the steady increase in the number of news articles, analyses, and Q-analyses published on the website over the years. This consistent linear growth may be interpreted as a reflection of the stable growth within the quantum industry itself, suggesting that the sector has yet to transition into a phase of exponential growth. As the quantum landscape continues to evolve, it will be fascinating to observe whether this linear trend persists or if we will witness a significant uptick in the rate of development and adoption in the coming years.

What are the conditions necessary for the quantum computing market to transition into exponential growth?

Global Quantum Intelligence has previously analyzed the challenges that quantum computing hardware must overcome, which include: code scaling for systematically suppressing logical errors, universal fault-tolerant circuits with realistic clock times, and platforms capable of scaling to commercially relevant sizes.

From a commercial perspective, there are several key indicators to watch for to ensure that opportunities are not missed as the technology rapidly scales:

(I) **Increased interest in resource estimation:** As hardware matures, companies will begin to assess whether the technology is sufficiently advanced to meet their needs. This heightened interest in resource estimation will be the first sign that an inflection point is approaching.

(II) **Quantum computing use cases moving into production:** A growing percentage of mature use cases that deliver daily commercial value will be a clear indicator of the market's readiness for exponential growth.

(III) **Technological advancements in use case algorithms:** From a technological standpoint, observing an increasing number of use cases based on algorithms with guarantees, ensuring that the value cannot be obtained through existing solutions, will be the final and most significant sign to watch for. Use cases leveraging fault-tolerant quantum computing (FTQC) primitives, such as Quantum Amplitude Amplification, Quantum Fourier Transform, or Grover's search, will be particularly indicative of this shift.

25. SafeLogic Announces Post-Quantum Cryptography (PQC) Early Access Program at RSA Conference 2024

by SafeLogic
https://www.prweb.com/releases/safelogic-announces-post-quantum-cryptography-pqc-early-access-program-at-rsa-conference-2024-302135418.html

SafeLogic today (06 May 2024) announced the launch of an Early Access Program (EAP) for its next-generation cryptographic software modules that include comprehensive support for all the PQC algorithms NIST is planning to standardize in the summer of 2024. Available now, these modules will allow

SafeLogic customers to test and experiment with PQC algorithms and capabilities such as cryptographic asset discovery, cryptoagility, and hybrid use cases. SafeLogic will be demonstrating these modules in booth #6572 at the RSA Conference 2024 in San Francisco this week.

Quantum computers are promising to offer many benefits to society, but the advent of that technology also carries some risks. One major risk is the threat that quantum computers are expected to pose to the world's public key (asymmetric) encryption. It is believed that once sufficiently powerful quantum computers are available, they will be able to break most of the widely available public key encryption in use today. Should this risk materialize, the significant negative impact on security, privacy, and trust is hard to overstate.

Correspondingly, NIST has been running a worldwide competition for over five years now to select and standardize PQC algorithms that are resistant to cryptanalytic attacks from future quantum computers. SafeLogic had been working closely with NIST and other industry collaborators on NIST's NCCOE PQC migration project where it had been leading the PQC migration prioritization workstream.

``For over a decade, SafeLogic has been a trusted and proven cryptographic software solutions partner for companies that require strong, FIPS 140 validated cryptographic software. Our customers include top technology vendors, many of which sell to regulated industries such as the US Public Sector that already have PQC migration requirements in place via various executive orders and congressional actions," said Evgeny Gervis, CEO of SafeLogic. "These and other customers, such as financial services and healthcare organizations, want to start preparing for PQC migration now, and SafeLogic is excited to be their partner on that journey.”

SafeLogic's PQC solutions offer several capabilities that organizations migrating to PQC will find important.

- PQC algorithms CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, SPHINCS+, LMS, and XMSS are now available for customer testing. SafeLogic expects to incorporate these into its FIPS 140 validated CryptoComply software once NIST completes the standardization process and doing so becomes possible.

- SafeLogic takes a unique approach to cryptographic asset discovery by providing real-time operational information for when quantum-vulnerable cryptography is being used. This information can greatly help organizations with their cryptographic inventories and migration prioritization decisions.

- SafeLogic's approach to cryptoagility builds on CryptoComply's provider architecture to reduce the effort required for future cryptography migrations.

- SafeLogic's approach to hybrid mode allows organizations to safely wrap classical FIPS 140-2 or FIPS 140-3 validated encryption in PQC to protect valuable data from "harvest now, decrypt later" attacks while maintaining FIPS compliance and providing defense in depth.

SafeLogic's PQC solutions offer several distinct advantages, including field-proven validated cryptographic implementations, extensive environment coverage with maximum compatibility, commercial-grade support, support for CNSA 2.0, and increasing implementation in memory-safe languages. As the world prepares for PQC migration, the largest migration in the history of cryptography, the dimensions above will be key to meeting their needs in a comprehensive fashion.

26.A Close Call: Lattice Cryptography Safe for Now

by David Joseph
https://www.sandboxaq.com/post/a-close-call-lattice-cryptography-safe-for-now?mkt_tok=MTc1LVVLUi03MTEAAAGTb10kAle_Pvq1NVHNs5AkBtTFmhjnojB9vykXMQxNbsCrRlf9rNLrj-FUMYWYikgg9zGRVDRs_EPMkpDmmDkGQh9k2FnR_Lv3B-qZPPZPn

Cryptography evolves

Organizations today depend on cryptography as the bedrock of their secure communications, providing integrity, authenticity, and confidentiality. Cryptography is often hard wired into each individual software application -- that's a big problem if you want to be nimble and update the encryption to more secure standards across many thousands of apps that make up modern IT infrastructure. This nimbleness is called *crypto-agility.*

Cryptography is evolving rapidly to counter hackers who are developing more sophisticated attacks. As security protocols are broken, companies need to replace and upgrade quickly. For example, one of the standard ways to protect password files – SHA1 – was shown to be vulnerable in 2005, but by the time it was ultimately broken in 2017 (12 years later), one in five websites still relied on it due to the difficulty of updating web certificates.

The recently claimed quantum attack against lattices

A paper released this month cast doubt on a new family of cryptography that many were counting on for the next generation of secure communications, which must be resistant to the threat posed by quantum computers.

The paper (in pre-print - i.e. not yet peer reviewed) reinvigorated discussions of crypto-agility by claiming that an efficient quantum algorithm solves a presumed hard computational problem closely related to three upcoming NIST Post-Quantum Standards for both key exchange and signatures. For over a week, foremost experts in quantum computing and lattice cryptography opined on the implications and pored over the proofs, even teaming up on Discord to quickly exchange ideas. Finally a mistake was identified in the proposed algo.

The bug identified in the paper does not appear to be easily fixed, thus lattice cryptography remains safe. The algorithms that could have been impacted have not yet been standardized, and as such are not now widely implemented. However, the prospect of relying on an alternative to lattice-based cryptography would have meant a significant shift in trajectory for standards bodies, academics, and security regulators.

Plan for cryptographic obsolescence

While the claimed result has not been proven out, this is a good reminder that almost all cryptography is based on computational problems that are only *presumed* to be hard. As these standards filter into production, it is critical to adopt modern cryptography management practices that ensure cryptographic agility and resilience.

Reflecting on the mortality of cryptography before it has even been deployed should urge us to put modern cryptographic best-practices at the forefront of system design. The best way to minimize the future costs of updating cryptography is to *plan for obsolescence even before algorithms are rolled out*. In the history of cryptography, few algorithms – and fewer implementations – have stood the test of time.

Adopting practices to monitor the deployment and usage of cryptography and move to a crypto-agile framework will raise the level of security of all companies and governments.

27.Get started with Qiskit SDK 1.0 at the 2024 IBM Quantum Challenge

by Brian Ingmanson and Vishal Sharathchandra Bajpe
https://www.ibm.com/quantum/blog/2024-quantum-challenge

This year's challenge starts on 5 June, and is about Qiskit SDK 1.0 and working toward utility-scale quantum experiments.

Earlier this year, we debuted the first stable release of the Qiskit SDK, the IBM software for programming utility-scale quantum computers. Now, we challenge you to put it to work.

We're excited to introduce the 2024 IBM Quantum Challenge. This annual coding challenge is an educational event focused on teaching the world how quantum computational scientists use Qiskit. This year's challenge is about Qiskit 1.0 and working toward utility-scale quantum experiments.

It will begin on 5 June and run until 14 June — Sign up here.

As with previous challenges, the 2024 IBM Quantum Challenge is tailored for anyone to join, regardless of their experience — whether you're a newcomer or a seasoned veteran, there is something here for you. It consists of a series of Jupyter notebooks that contain tutorial material, code examples, and auto-graded coding challenges. We call each of these notebooks a "lab." While the first lab can be completed by beginners, the final labs will test your Qiskit knowledge. This is, after all, a challenge!

This year's challenge will showcase the new features of Qiskit 1.0, while demonstrating the differences from previous versions. We hope it will help you better understand what it means to do utility-scale experiments with Qiskit — those with 100 or more qubits — and practice the steps to get there.

This challenge is also an opportunity to get a sneak peek at some of the new cutting-edge features and developments in the quantum stack. That includes new integrations with AI — the Qiskit code assistant powered by IBM watsonxTM.

We're also making some changes to accommodate our ever-growing quantum community. Events like this typically attract thousands of users running the same circuits multiple times, making queue times much longer than normal. Therefore, we will not be requiring hardware use as part of the Quantum Challenge. The labs in this year's Challenge will focus on helping people to build intuition and make progress without waiting to run on real hardware.

However, as always, you are encouraged to run any of the code here on any of our devices which you have access to — such as those available through the IBM Quantum Open, Pay-as-you-go, or Premium Plans. That's the beauty of IBM's offerings, you can easily transition your code from testing straight to

running on actual hardware.

The workflow you'll learn in this challenge is a shift away from IBM Quantum Lab, which will be sunset on 15 May, to focus on utility-scale workloads. We will offer tutorial content and hands-on support to assist you with this new workflow.

