Crypto News

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

May 01, 2024

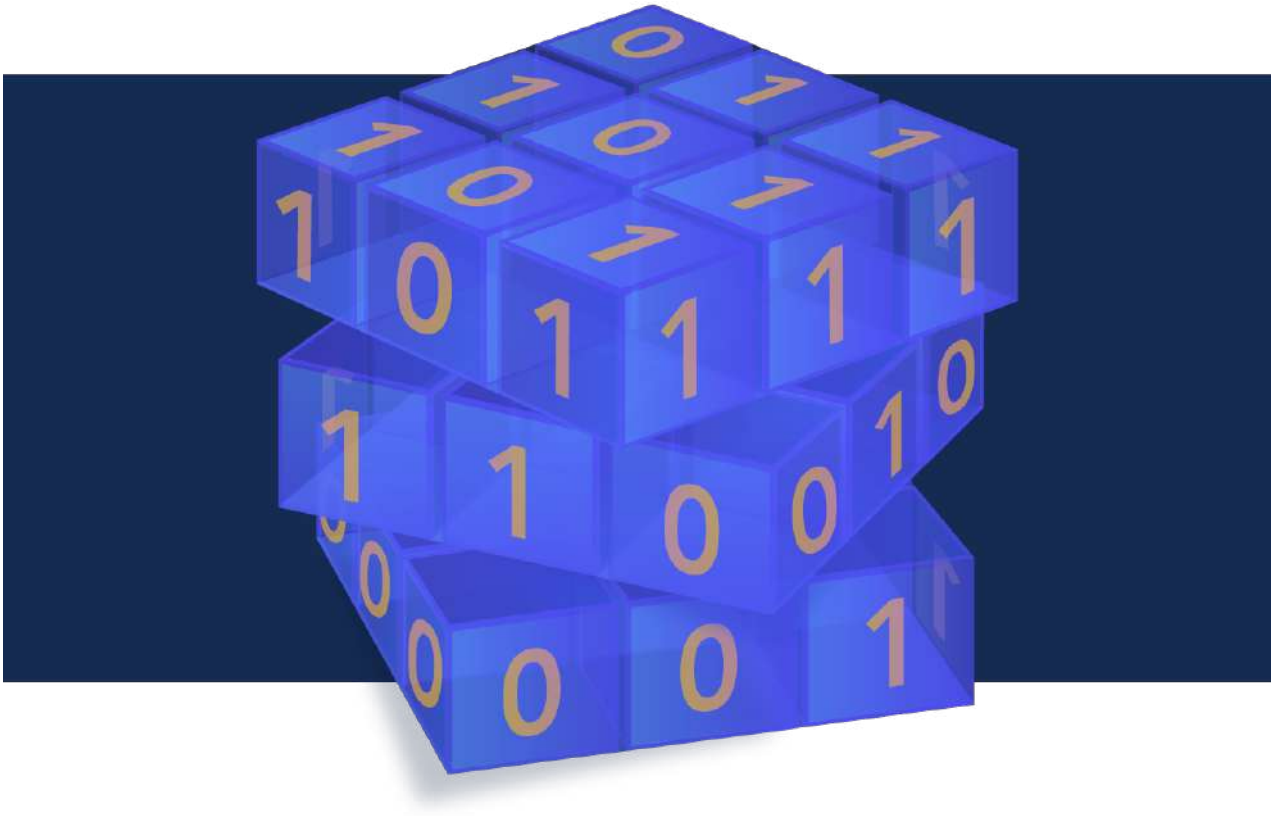


TABLE OF CONTENTS

1.THE QUANTUM COUNTDOWN: EXPERT URGES FOR THE POST-QUANTUM CRYPTOGRAPHY SOLUTION 5

2.KEYSIGHT INTRODUCES NEW TESTING CAPABILITIES TO STRENGTHEN POST-QUANTUM CRYPTOGRAPHY 6

3.FULLY HOMOMORPHIC ENCRYPTION CAN REVOLUTIONIZE EDUCATION 7

4.GOOGLE CHROME'S NEW POST-QUANTUM CRYPTOGRAPHY MAY BREAK TLS CONNECTIONS 8

5.DENMARK'S STRATEGIC MOVE TO LEAD GLOBAL QUANTUM INNOVATION 10

6.EXISTING BLOCKCHAINS CAN'T ADOPT POST-QUANTUM CRYPTOGRAPHY WITHOUT SIGNIFICANT USER IMPACT, SAYS JOHANN POLECSAK 11

7.THREE WAYS AI IS TRANSFORMING CLOUD SECURITY, ACCORDING TO EXPERTS 14

8.CHINA LAUNCHES 504-QUBIT QUANTUM CHIP, OPEN TO GLOBAL USERS 17

9.CAN WE BALANCE SECURITY AND PRIVACY? THOUGHTS 10 YEARS AFTER SNOWDEN 17

10.QUANTUM RANDOM NUMBER GENERATION TECHNOLOGY MADE AVAILABLE TO THOUSANDS OF BUSINESSES WORLDWIDE 19

11.TOHOKU UNIVERSITY-LED RESEARCH TEAM ACHIEVES ROOM-TEMPERATURE QUANTUM-METRIC MANIPULATION 21

12.DECRYPTING THE FUTURE: PROGRAMMABLE CRYPTOGRAPHY AND ITS ROLE IN MODERN TECH 22

13.A WEAKNESS IN ONE OF THE NIST PQC ALGORITHMS WAS NOT UNCOVERED AFTER ALL 24

14.BREAKTHROUGH IN QUANTUM CLOUD COMPUTING ENSURES ITS SECURITY AND PRIVACY 25

15.UNBREAKABLE TRUST: SAFEGUARDING BRANDS WITH THE POWER OF CRYPTOGRAPHIC SIGNATURES 29

16.LOCAL QUBIT CONTROL BRINGS NEW CAPABILITIES TO QUERA'S QUANTUM COMPUTER 30

17.D-WAVE INTRODUCES NEW FAST ANNEAL FEATURE, EXTENDING QUANTUM COMPUTING PERFORMANCE GAINS 32

18.PREPPING FOR POST-QUANTUM CRYPTOGRAPHY 33

19.QUANTINUUM SETS NEW RECORDS FOR BOTH GATE FIDELITY AND QUANTUM VOLUME 35

20.QUNNECT ACHIEVES RECORD-BREAKING PERFORMANCE FOR DISTRIBUTING POLARIZATION QUBITS ON GOTHAMQ NETWORK IN NYC 36

21.WORLD QUANTUM DAY — PUTTING THE 'WORLD' BACK IN WORLD QUANTUM DAY 38

22.QUANTUM XCHANGE JOINS MIGRATION TO POST-QUANTUM CRYPTOGRAPHY PROJECT CONSORTIUM 41

23.MEPS CALL FOR 'URGENT ACTION' TO IMPLEMENT POST-QUANTUM ENCRYPTION STANDARDS 42

24.POST-QUANTUM CRYPTOGRAPHY GETS PERFORMANCE TESTING CAPABILITY 43

25.VIAVI INTRODUCES PERFORMANCE TESTING FOR POST-QUANTUM CRYPTOGRAPHY DEPLOYMENTS 44

26.EU COMMISSION ADVOCATES FOR POST-QUANTUM CRYPTOGRAPHY ADOPTION 45

27.POST-QUANTUM CRYPTOGRAPHY (PQC) 47

28.LIVE QKD DEMONSTRATIONS AT OFC CONFERENCE 50

Editorial

Dear Readers,

Here is your expected Newsletter from the QSS working group, with admittedly some delay (as some of you may know, May is the “best” month in Europe, due to the numerous holidays… Hard to have any serious work done…).

As usual, there are many interesting articles and it is hard to make a choice. Just check all of them!

However, since I have to provide some guidance, I recommend a deeper look at 3 and 14, because I see them as twins, which provide classical and quantum solutions to a significant issue, which is truly relevant to Cloud Computing.

Number 3 discusses Fully Homomorphic Encryption (FHE), which is a way to do computation directly on encrypted data (for example stored in the cloud). With FHE, a cautious user can send her/his data to the cloud in an encrypted form, and could still perform any kind of computation, without having to disclose the data to the cloud provider or anybody else. FHE is a classical solution, which is still computer intensive and in the development stage.

An alternative quantum solution is explained in Number 14. It is named Blind Quantum Computing (BQC). With BQC, a user could ask a remote quantum computer to perform a computation for her/him, without disclosing the details of the computation. The most significant contribution I see is that all the quantum complexity is at the server, The end user only needs to have single photon detector and an optical fiber connection to the quantum server. In the long run, we can envisage a quantum computer cloud, offering computation services to end users, without knowing anything on the computation they perform.

Interesting to see two totally different concepts, one classical and one quantum, aiming to offer something like computing privacy in the cloud. Quantum and classical solutions should indeed complement each other.

Thanks to Dhananjoy for his thorough reading of current crypto news. And a good reading to all.

The Crypto News editorial is authored by the Chair of the Quantum-Safe SecurityWorking Group (QSS WG) of the Cloud Security Alliance (CSA), Bruno Huttner, Director of Strategic Quantum Initiatives at ID Quantique SA and it is compiled by Dhananjoy Dey. Both are active members of the CSA QSS WG. The guiding principle of the QSS WG is to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting their networks and their data.

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

1.The Quantum Countdown: Expert Urges for the Post-Quantum Cryptography Solution

by James Dargan
https://thequantuminsider.com/2024/04/30/the-quantum-countdown-expert-urges-for-the-post-quantum-cryptography-solution/

A leading expert in cryptography and computer security at the cutting edge of preparing for the quantum computing era, Nigel Smart is a professor at COSIC at the Katholieke Universiteit Leuven and Chief Academic Officer at Zama. A cryptographer by profession, Smart is working to future-proof our digital information against the potential security threats posed by powerful quantum computers.

Smart recently explained during a video series, much of modern cryptography relies on the difficulty of factoring large numbers into their prime components: “Everyone’s heard of the factoring problem—if you multiply two prime numbers together it’s easy to do multiplication but it’s hard to split them into primes again. It’s a very old form of cryptography.”

However, he warns “if a sufficiently large quantum computer was ever built, it would be able to break the cryptography that we use on the internet today.” Quantum computers could render many current encryption methods obsolete by rapidly factoring large numbers.

The solution, according to Smart, is “post-quantum cryptography” which “takes the factoring problem, for example, and replaces it with a problem that not even quantum computers can break. It’s still a hard mathematical problem, but it’s harder in the sense that quantum computers are not able to break it.”

Smart stresses that “companies should actually be anticipating that in the next five to ten years they will need to replace their existing solutions with ones which are post-quantum secure.”

A key challenge is having the “crypto agility” to transition systems to new post-quantum cryptographic algorithms.

“You need to consider the problem—am I crypto agile? Am I able to respond quickly if there is a problem found with an algorithm and switch out and put a new one in?” Smart noted.

Businesses must take stock of their “crypto assets” and prepare migration paths, understanding “what algorithms you’re using and when, what keys are you using and when” across the whole organization.

The urgency of migrating to quantum-safe encryption depends on the lifespan of sensitive data. Smart explains that even if a quantum computer is still years away.

“You could be creating a document that you want to be secure in 10 years time, like a will,” he said. Companies must “estimate when you think a quantum computer will come along” and start using post-quantum crypto for longterm sensitive documents before that point.

While the “standards are only out” recently, Smart advises proactively developing a “risk profile” rather than panic, matching the estimated quantum computing timeline against your sensitive data longevity

needs. Most companies can take measured steps “preparing a migration path probably over the next five or six years.”

2.Keysight Introduces New Testing Capabilities to Strengthen Post-Quantum Cryptography

by Paul Erwin
https://www.businesswire.com/news/home/20240430030207/en/

Keysight Technologies, Inc., has announced an industry-first automated solution designed to test the robustness of post-quantum cryptography (PQC). This latest addition to Keysight Inspector is a notable expansion of the comprehensive platform that helps device and chip vendors identify and fix hardware vulnerabilities.

Quantum computing is designed to substantially accelerate complex calculations. This development will inevitably threaten existing encryption technologies. Algorithms like RSA and ECC, proven and robust in the current conventional computing era, could be easily circumvented. As the industry looks to remain resilient both now and in the future, this means developing new PQC encryption algorithms. This will be important for applications where encrypted data is captured on the assumption it can be decrypted later. However, new technologies assumed to be resilient against post-quantum attacks may be vulnerable to existing hardware-based attack methods.

Keysight Inspector, part of the company’s recently acquired device security research and test lab Riscure, addresses this challenge. The Keysight Inspector device security testing platform can now be used to test the implementations of the Dilithium algorithm, one of the PQC algorithms selected by NIST. For adopters of this algorithm in hardware, this allows designers to verify that products are secure against these threats. The test solution will also be necessary for government institutions and security test labs that want to verify the strength of third-party products.

With ongoing standardization, Keysight expects dozens of new security algorithms to become available for multiple applications and industries. Ultimately, these algorithms will need verifiable implementations. Keysight will provide the necessary test tooling in addition to certification services through Keysight Inspector.

In addition, Keysight Inspector can also test the chips and analyze the silicon design before implementation by simulating the hardware code pre-silicon. Riscure has been working with PQShield, the leading developer of PQC solutions, to conduct both pre- and post-silicon analyses of their products.

Dr Axel Poschmann, Vice President of Product at PQShield, said: “Keysight will help us verify the robustness of our implementations at an early stage. Building on our original work with Riscure within the Keysight portfolio is exciting and we are looking forward to continuing this journey.”

Marc Witteman, Director of the Device Security Research Lab at Keysight, said: “Post-quantum resilience does not guarantee total security. We have observed incidents when the latest post-quantum encryption technology suffers from hardware-based threats. With this technology being implemented at a larger scale, the need for comprehensive testing becomes apparent. We are addressing this need by

adding post-quantum algorithm testing capability to the Keysight Inspector solution, our comprehensive device security testing platform."

Keysight will provide live demonstrations of the Keysight Inspector hacking a PQC implementation running on a popular processor at booth 4418 during the upcoming RSA Conference in San Francisco.

3.Fully Homomorphic Encryption can revolutionize education

by Jeremy Bradley
https://www.ecampusnews.com/it-leadership/2024/04/29/fully-homomorphic-encryption-revolutionize-higher-education/

Fully Homomorphic Encryption (FHE) is a revolutionary cryptographic technique that allows for computations to be performed on encrypted data without needing to decrypt it first. Imagine you have a secret message inside a locked box, and you want someone to do some math with that message without seeing what's inside. FHE is the magic that lets them do the math on the box without opening it, and when they're done, the secret message inside the box has changed according to the math, but it's still a secret.

This groundbreaking technology has the potential to significantly impact various sectors, including education, by offering new ways to handle data securely and privately. Let's explore the implications of FHE for the education sector, focusing on its benefits, potential applications, and challenges.

Benefits of FHE in education

1. **Enhanced data privacy:** In an era where educational institutions hold vast amounts of sensitive data, including student records, personal information, and academic research, FHE offers an unprecedented level of security. By enabling computations on encrypted data, it ensures that the information remains confidential, even from the operators of the data infrastructure.

2. **Secure cloud services:** FHE facilitates the use of cloud-based educational tools and resources by ensuring that data can remain encrypted while being processed. This means that schools and universities can leverage cloud computing without compromising the privacy and security of their data.

3. **Collaborative research with privacy:** Academic institutions often collaborate on research projects that involve sensitive data. FHE allows researchers to compute on data jointly without revealing their inputs to each other, fostering collaboration while safeguarding privacy.

Potential applications of FHE in education

1. **Secure online examinations:** FHE can ensure the integrity and confidentiality of online tests and exams by encrypting answers and grading scripts. This application could dramatically reduce the risk of cheating and unauthorized access to exam content.

2. **Private student analytics:** Educational institutions can use FHE to analyze student performance data without exposing individual records. This enables personalized education plans and interventions while protecting student privacy.

3. **Confidential surveys and feedback:** FHE can secure the process of collecting and analyzing surveys, feedback, and other sensitive information, ensuring that responses remain confidential and tamper-proof.

4. **Secure sharing of educational resources:** Publishers and educational content providers can use FHE to offer secure, encrypted educational materials that can be accessed and utilized without exposing the content to unauthorized users.

Challenges and considerations

Despite its promising applications, FHE is not without challenges. The primary issue is the computational complexity and the resulting performance overhead. FHE operations are currently significantly slower than operations on unencrypted data, which could limit its practicality for real-time applications or large datasets. Moreover, the technology is still in the development phase, requiring further research and innovation to become widely accessible and cost-effective.

Furthermore, the implementation of FHE requires expertise in cryptography and security, which might be a barrier for educational institutions without the necessary resources or knowledge. As such, there is a need for user-friendly tools and platforms that can facilitate the adoption of FHE in the education sector.

Fully Homomorphic Encryption holds the promise of transforming the education sector by offering a new paradigm for secure and private data handling. Its potential to enhance data privacy, enable secure cloud services, and facilitate confidential collaborative research could lead to significant advancements in educational technologies and methodologies. However, realizing the full potential of FHE requires overcoming technical challenges and making the technology more accessible to educators and researchers. With continued development and adoption, FHE could play a crucial role in the future of education, where data security and privacy are paramount.

4.Google Chrome's new post-quantum cryptography may break TLS connections

by Sergiu Gatlan
https://www.bleepingcomputer.com/news/security/google-chromes-new-post-quantum-cryptography-may-break-tls-connections/

Some Google Chrome users report having issues connecting to websites, servers, and firewalls after Chrome 124 was released last week with the new quantum-resistant X25519Kyber768 encapsulation mechanism enabled by default.

Google started testing the post-quantum secure TLS key encapsulation mechanism in August and has now enabled it in the latest Chrome version for all users.

The new version utilizes the Kyber768 quantum-resistant key agreement algorithm for TLS 1.3 and QUIC connections to protect Chrome TLS traffic against quantum cryptanalysis.

"After several months of experimentation for compatibility and performance impacts, we're launching a hybrid postquantum TLS key exchange to desktop platforms in Chrome 124," the Chrome Security Team explains.

"This protects users' traffic from so-called 'store now decrypt later' attacks, in which a future quantum computer could decrypt encrypted traffic recorded today."

Store now, decrypt later attacks are when attackers collect encrypted data and store it for the future when there may be new decryption methods, such as using quantum computers or encryption keys become available.

To protect against future attacks, companies have already started to add quantum-resistant encryption to their network stack to prevent these types of decryption strategies from working in the future. Some companies that have already introduced quantum-resistant algorithms include Apple, Signal, and Google.

However, as system admins have shared online since Google Chrome 124 and Microsoft Edge 124 started rolling out on desktop platforms last week, some web applications, firewalls, and servers will drop connections after the ClientHello TLS handshake.

The issue also affects security appliances, firewalls, networking middleware, and various network devices from multiple vendors (e.g., Fortinet, SonicWall, Palo Alto Networks, AWS).

"This appears to break the TLS handshake for servers that do not know what to do with the extra data in the client hello message," one admin said.

"Same problem here since version 124 of Edge, it seems to go wrong with the SSL decryption of my palo alto," said another admin.

These errors are not caused by a bug in Google Chrome but instead caused by web servers failing to properly implement Transport Layer Security (TLS) and not being able to handle larger ClientHello messages for post-quantum cryptography.

This causes them to reject connections that use the Kyber768 quantum-resistant key agreement algorithm rather than switching to classic cryptography if they don't support X25519Kyber768.

A website named tldr.fail was created to share additional information on how large post-quantum ClientHello messages can break connections in buggy web servers, with details on how developers can fix the bug.

Website admins can also test their own servers by manually enabling the feature in Google Chrome 124 using the chrome://flags/#enable-tls13-kyber flag. Once enabled, admins can connect to their servers and see if the connection causes an "ERR_CONNECTION_RESET" error.

How to fix connection issues

Affected Google Chrome users can mitigate the issue by going to chrome://flags/#enable-tls13-kyber and disabling the TLS 1.3 hybridized Kyber support in Chrome.

Administrators can also disable it by toggling off the PostQuantumKeyAgreementEnabled enterprise policy under Software > Policies > Google > Chrome or contacting the vendors to get an update for servers or middleboxes on their networks that aren't post-quantum-ready.

Microsoft has also released information on how to control this feature via the Edge group policies.

However, it's important to note that long-term, post-quantum secure ciphers will be required in TLS,

and the Chrome enterprise policy allowing disabling it will be removed in the future.

"Devices that do not correctly implement TLS may malfunction when offered the new option. For example, they may disconnect in response to unrecognized options or the resulting larger messages," Google says.

"This policy is a temporary measure and will be removed in future versions of Google Chrome. It may be Enabled to allow you to test for issues, and may be Disabled while issues are being resolved."

5.Denmark's Strategic Move to Lead Global Quantum Innovation

by Matt Swayne
https://thequantuminsider.com/2024/04/26/tqi-exclusive-denmarks-strategic-move-to-lead-global-quantum-innovation/?utm_source=newsletter&utm_medium=email&utm_term=2024-04-27&utm_campaign=TQI+Weekly+Newsletter+--+Xanadu+Is+On+The+Chica+go+Neutral+Atom+Partnership+Plus+More+Quantum+News+Industry+Updates

Deep Tech Lab – Quantum (DTL-Q), an ambitious accelerator, aims to position Denmark as a significant player in the global quantum technology sector. The accelerator seeks to leverage Denmark's research strengths and strategic partnerships to carve out a place on the international stage.

Holistic Approach to Startup Success

At DTL-Q, the support for startups extends beyond funding. The accelerator cultivates a comprehensive ecosystem that nurtures all aspects of startup growth—from securing venture capital to navigating the complexities of public and private funding landscapes.

Cathal Mahon, Chief Business Officer at Deep Tech Lab Quantum, emphasized the breadth of this support, "We're building an ecosystem that does more than just fund; we're creating a community that supports all facets of a startup's development."

The infrastructure around DTL-Q is meticulously designed to cater to the specialized needs of quantum technologies. Through close collaboration with nearby universities, such as the renowned Niels Bohr Institute at the University of Copenhagen, the facilities are tailored to foster innovation and expedite the journey from concept to market.

DTL-Q's strategy includes forging key partnerships to expand its reach and resources. A notable collaboration is with the Defence Innovation Accelerator for the North Atlantic (DIANA), which connects startups to an extensive network of investors, testing facilities, and expert mentorship.

"Our role in DIANA amplifies our capacity to support dual-use innovations that have both civilian and defense applications," Mahon said.

This involvement not only enhances the support available to DTL-Q's startups but also underscores Denmark's strategic role in the broader tech ecosystem.

From Life Sciences to Quantum Breakthroughs

DTL-Q's origins trace back to the BioInnovation Institute, an initiative by the Novo Nordisk Foundation aimed at bridging the gap between academic research in life sciences and its commercial application. Observing similar opportunities in the quantum sector, the foundation adapted its approach to catalyze the commercialization of quantum research.

Reflecting on this transition, Mahon said, "A lot of investment was made into basic research, but there wasn't much visible impact in terms of startups."

Mahon draws a compelling parallel between the fields of life sciences and quantum technologies, both characterized by high costs, long development times, and substantial risks.

"When you're working with life science companies, particularly in therapeutics, and similarly with quantum computing, the parallels are clear. Both fields require a lot of time, involve high risks, and demand interdisciplinary teams adept at handling complex technological challenges," said Mahon. "This way of thinking is totally ingrained in the way that people work with the companies and the processes that they have. So essentially, that is what we're building upon here at DTL-Q."

Looking Forward

Looking forward, Mahon expresses cautious optimism about DTL-Q's future.

"We aim to position ourselves among the top global accelerators, but we recognize the competitiveness of the field and the inherent challenges," he said.

DTL-Q seeks to utilize its strong foundations in research and its understanding of market dynamics to achieve its goals.

As the technology landscape evolves, DTL-Q aims to enhance Denmark's stature in the quantum field thoughtfully and strategically. By fostering international collaborations and building a supportive ecosystem, DTL-Q hopes to contribute to the development of future industry leaders in quantum technology.

Deep Tech Lab – Quantum represents Denmark's commitment to advancing quantum technologies. By providing comprehensive support and fostering international partnerships, DTL-Q participates actively in the global quantum innovation race, aiming to influence the future of this emerging technological frontier effectively.

6.Existing Blockchains Can't Adopt Post-Quantum Cryptography Without Significant User Impact, Says Johann Polecsak

by Terence Zimwara
https://news.bitcoin.com/existing-blockchains-cant-adopt-post-quantum-cryptography-without-significant-user-impact-says-johann-polecsak/#google_vignette

As the prospect of quantum computers breaking today's cybersecurity standards edges ever closer, Jo-

hann Polecsak, co-founder of the QAN blockchain platform, argues that public blockchains such as Bitcoin, Ethereum, and Solana are still ill-equipped to adopt post-quantum cryptography without significant user impact.

Post-Quantum Migration Risks

Polecsak, an advocate for heightened awareness of imminent quantum attacks, asserts that the pseudonymity of blockchain will backfire during post-quantum migration. In written answers sent to Bitcoin.com News, Polecsak explained that this occurs because it will be impossible to distinguish legitimate crypto asset owners moving their funds and data from hackers attempting to steal the funds.

With billions of dollars likely to be lost, rendering the aforementioned public blockchains worthless, Polecsak said attempting a rescue is already a lost cause. He added that there is simply no secondary authentication mechanism to prevent this from happening in the case of already running blockchains.

Polecsak suggested that Google's quantum computing breakthrough in 2019 should serve as a wake-up call to enterprises and governments. They can no longer neglect the threat of quantum computing attacks if they want to protect their cybersecurity infrastructure. For individual users who do not wish to lose their funds, Polecsak advised that they must conduct their research to find the right time to transfer their assets to a post-quantum blockchain.

Elsewhere, the QAN blockchain co-founder also explained why it is no longer the time to focus on whether quantum computing can break blockchain security algorithms. He briefly discussed how his platform is tackling the threat of quantum attacks.

Below are Polecsak's answers to all the questions sent.

Bitcoin.com News (BCN): What are quantum computing attacks, and what threat do they pose to blockchains and cryptocurrencies? How long will it be before quantum computers are capable of breaking the security algorithms in blockchains?

Johann Polecsak (JP): Powerful quantum computers with sufficient stable qubits will be able to break today's cybersecurity standards. Today's asymmetric cryptographic algorithms like RSA and EC used by the whole internet – including governments, banks, email providers, social media, blockchain platforms, etc .– will be cracked by quantum computers.

This threat affects blockchain technology as follows: all cryptocurrency wallets relying on Elliptic Curve (EC) cryptography which have at least one outgoing transaction will break. In short: hackers will be able to steal your cryptocurrency.

We are already having the wrong conversation in cryptography if we argue about whether we have 1, 3, or 5 years before quantum computers will break today's security algorithms. We must always be ahead of the curve when it comes to cybersecurity.

BCN: How challenging would it be for blockchain projects as well as centralized enterprises or governments to make their infrastructure quantum-resistant? Blockchains tend to be fairly decentralized so how would this affect their ability to embrace post-quantum cryptography?

JP: Currently, only a limited number of companies and cryptographers are comfortable with post-quantum cryptography and cybersecurity, but for the sake of this discussion, let's set that aspect aside.
Centralized authorities like governments, companies, and organizations can switch their IT security to post-quantum cryptography much more easily than blockchain platforms. People often overlook that blockchains are decentralized.

Existing public blockchains like Bitcoin, Ethereum, Solana, etc. cannot adopt post-quantum cryptography without significant user impact. According to Vitalik Buterin: “few users would lose their funds”. Pseudonymity of blockchain will backfire at post-quantum migration because it will be impossible to tell legitimate owners migrating their own funds and data or hackers stealing all of it apart. In this case, billions of dollars worth of “free money” and data could land in hackers’ hands if they start migrating on the real owners’ behalf making the affected blockchains immediately worthless. There is simply no secondary authentication mechanism to prevent this from happening in case of already running blockchains.

BCN: Could you explain the quantum-resistant technology of Qanplatform, its workings, and the cryptography it employs to safeguard networks from future quantum attacks? How does the technology of Qanplatform integrate with existing blockchains?

JP: We are developing a quantum-resistant hybrid blockchain. We already released the first version of the QAN Private Blockchain or so called QAN Enterprise Blockchain last year. We will launch the quantum-resistant QAN TestNet this spring.

In alignment with the US National Institute of Standards and Technology (NIST)’s primary recommendations, QAN blockchain platform has incorporated CRYSTALS-Dilithium algorithm into QAN XLINK. Actually QAN has been using CRYSTALS-Dilithium well before NIST started recommending it as the primary PQ signature algorithm. The QAN XLINK cross-signer ensures post-quantum transaction security while maintaining Ethereum EVM compatibility, safeguarding the QAN blockchain platform and its users against the looming threat of quantum computing.

This protocol enables seamless integration of every Ethereum-compatible wallet (such as MetaMask, Trust Wallet, and Ledger) with Quantum-resistant signature-capable keypairs. Operated on the blockchain, XLINK runs as a lightweight, continuous process that can be effortlessly deployed currently on desktop, operating in the background. Your transactions are only approved when accompanied by a corresponding XLINK signature linked to your wallet, authenticated with a post-quantum key. With this unique approach there’s no need for draconian measures like cutting off funds for those who fail to migrate to post-quantum crypto promptly. Nor do we face unnecessary risks posed by quantum computing attacks, which could potentially flood the market and disrupt the economics of most chains.

BCN: Big tech companies like Apple, Google, Microsoft and others may well have their initiatives developing quantum computers. However, is it also possible that they are also working on countermeasures to protect against quantum attacks?

JP: Each of the three IT giants is somewhat involved in quantum computing. Google, among the companies mentioned, is particularly active in this area, covering a wide spectrum, including quantum computing development and quantum-resistant security. Thanks to Google’s quantum computing achievement in 2019, the blockchain community became more aware of the upcoming threat posed by these powerful new machines to blockchain technology.

The past year has shown that everyone should prepare for the quantum threat. Microsoft launched its Quantum-Safe program, and Google and Apple have also taken a proactive approach by incorporating post-quantum cybersecurity into Google Chrome and Apple iMessage.

BCN: Recently, your platform announced that a country in Europe has adopted your quantum-resistant technology. While you have not disclosed the country’s name due to “national security reasons,” could you share with our readers how this country might be using your technology to secure its operations?

JP: Governments and critical infrastructures are currently the most exposed to ‘Store now, decrypt later’ cybersecurity attacks. Store now, decrypt later (SNDL) also known as harvest now, decrypt later (HNDL)

is a cybersecurity threat that involves attackers collecting encrypted data today, with the intention of decrypting it later using more powerful computing methods, such as quantum computers.

Essentially, attackers are capturing and storing the encrypted data now, knowing that they are highly likely to be able to decrypt it later as soon as technology advancements allow them to. I would be happy to share more information about how the first European country implemented QAN's technology; however, I haven't received approval to disclose any further details.

BCN: Earlier this year, the North Atlantic Treaty Organization (NATO) and the World Economic Forum related their strategies to prepare for the quantum era. The European Commission reportedly has a $1.07 billion (€1 billion) research initiative focused on quantum threats. What does this all mean for the individual users of the digital and blockchain platforms?

JP: It's no wonder why global powers are investing heavily in this technology—both in developing quantum computers and in enhancing security against them. Both are crucial in terms of cybersecurity from an offensive and defensive point of view.

Nevertheless, it must be highlighted that no matter how much these entities invest in these areas, their goal is not about saving already running public blockchains in particular, since that pretty much can not be even done as discussed above.

Individual users of blockchain platforms must do their own research to find the right time when to transfer their assets to a post-quantum blockchain to ensure their funds are secured against new, continuously evolving quantum computing attacks.

7.Three ways AI is transforming cloud security, according to experts

by Alissa Irei
https://www.techtarget.com/searchsecurity/tip/Ways-AI-is-transforming-cloud-security-according-to-experts

AI appears poised to revolutionize cybersecurity, with changes already happening on the ground -- and in the cloud.

In a recent survey by the Cloud Security Alliance (CSA) and Google Cloud, 67% of IT and security professionals said they have started testing generative AI (GenAI) capabilities for security use cases, with another 27% in the planning phase. Just 6% of respondents said they have no current plans to explore AI for security.

Experts say GenAI will increasingly augment cybersecurity operations, offering guidance and assistance to human practitioners to help them make better and more informed decisions. "That's especially relevant in cloud because cloud is complicated, dynamic and changes constantly," said Charlie Winckless, analyst at Gartner. "Staying on top of all of that is a problem."

It's a problem AI and machine learning (ML) promise to help solve, with natural language queries and responses already becoming a "standard staple" in cloud security tools, according to Andras Cser, analyst at Forrester.

The ability to ask a large language model (LLM) a question and receive a straightforward answer -- based on massive amounts of complex technical data, which AI models can process at speed -- is a potential game changer. Rather than sifting through the data themselves, practitioners can theoretically validate their decisions and harden an organization's security posture much more quickly and easily.

"Instead of having to really dig in and understand the details, we can ask natural language questions to sort through the noise of these tools more effectively and understand what's really happening," Winckless said.

Caleb Sima, chair of CSA's AI Safety Initiative, predicted AI will eventually autonomously construct and oversee cloud infrastructure and pipelines, automatically integrating sophisticated security controls to minimize the attack surface. In the short term, he added, AI-driven tools are already simplifying the cloud engineer's role by easing longstanding cloud security pain points.

Three key AI cloud security use cases

Key cloud security use cases for GenAI, according to experts, include the following.

1. Misconfiguration detection and remediation

Cloud misconfigurations pose one of the most serious security risks enterprises face, according to the CSA, National Security Agency, European Union and others.

In complicated cloud environments, settings and permissions errors perennially abound, opening the door to cyberattacks and the exposure of sensitive data. "At the end of the day, misconfigurations are behind a host of security breaches," Sima said.

Manually identifying and troubleshooting every cloud misconfiguration is time-consuming and tedious, if not impossible. AI tools can automatically analyze infrastructure and systems to detect anomalies and misconfigurations and then fix them. "They can automate remediation far faster and more efficiently than people can," Sima added.

In most cases today, however, AI tools likely suggest policy or configuration changes to human operators, who then approve or reject them, according to Winckless. While GenAI technology might be capable of independently remediating vulnerabilities without human intervention, it remains rare that security programs allow it to do so in real-world cloud environments.

"Most organizations are still unwilling to automate changes in development and production," Winckless said. "That has to change at some point, but it's about trust. It will take years." For the foreseeable future, he added, human oversight and validation of AI remain important and advisable.

2. User behavior analysis

Cser said he expects to see GenAI improve detection capabilities in cloud security, with the technology able to process huge data sets and identify unusual access patterns that human operators otherwise miss.

"AI will be able to take security teams on a deep dive into user behavior by contextualizing activities within the broader context of cloud environments," Sima agreed. AI algorithms will become increasingly good at recognizing abnormal behavior and alerting teams to potential security incidents, he added, based on factors such as the following:

- User roles.
- Access privileges.
- Device characteristics.
- Network traffic patterns.

Ultimately, Sima predicted, AI will not only be capable of accurately anticipating current user behavior, but future behavioral trends as well. "When taking this in total, we'll see AI being used to shape adaptive security policies and controls and assign risk scores to individual behaviors," he said.

3. Threat detection and response

Experts also anticipate GenAI will help security teams identify malware and other active cyberthreats much faster and more accurately than human practitioners can on their own by analyzing the real-time environment and cross-referencing it with threat intelligence data.

Already, GenAI-based investigation copilots are aiding security teams' threat response efforts, according to Cser, by recommending proactive measures based on activity patterns.

AI cloud security threats

Advancements in AI technology will also change the threat landscape, with increasingly sophisticated, AI-based attacks all but inevitable, according to experts. "Threat actors will be able to leverage AI algorithms to launch highly adaptive attacks and evasion techniques," Sima said.

This would be cause for greater concern, except that research indicated the vast majority of organizations are moving quickly to invest in defensive AI capabilities. "We can assume companies are already anticipating how to best use AI to stay one step ahead of threat actors," Sima said. He added, however, that organizations need to continually prioritize AI security investments going forward if they are to gain and maintain the upper hand.

In other words, the endless game of whack-a-mole in which defenders and attackers have long engaged appears likely to continue -- albeit heightened by GenAI and ML.

Getting started with AI-driven cloud security

Many cloud security vendors are building GenAI capabilities directly into their existing tools and platforms. That means all but the largest hyperscale organizations needn't -- and shouldn't -- worry about building their own AI models, according to Winckless.

But just because a provider rolls out GenAI capabilities doesn't mean they are infallible, or even necessarily ready for prime time. For example, users might encounter challenges such as AI hallucinations, in which an LLM produces erroneous information, which could be catastrophic in cybersecurity.

"Look at what frameworks your provider is using for generative AI and if they're providing any validation or verification of inputs and outputs," Winckless advised. "This is still an emerging space. It's very exciting, but it's also very challenging to determine how well the technology is being used."

8.China launches 504-qubit quantum chip, open to global users

by Xinhua
https://www.shine.cn/biz/tech/2404251668/

The Center for Excellence in Quantum Information and Quantum Physics under the Chinese Academy of Sciences has delivered a 504-qubit superconducting quantum computing chip to QuantumCTek, a leading quantum company based in east China's Anhui Province, setting a record for the number of qubits in a superconducting quantum chip in China, QuantumCTek said on Thursday.

The chip, "Xiaohong," is used to verify the kilo-qubit measurement and control system independently developed by the company, according to QuantumCTek.

The measurement and control system and the quantum computing chip are the core hardware of quantum computers, and the measurement and control system will greatly influence the overall performance of quantum computers, said Liang Futian, an associate professor at the center.

Liang said that the chip's key indicators, including the lifetime of its qubits, its gate fidelity and the depth of its quantum circuit, are expected to reach the chip performance levels of main international cloud-enabled quantum computing platforms such as IBM.

Gong Ming, a researcher at the center, said that the main purpose of the chip is to promote the development of large-scale quantum computing measurement and control systems, rather than to aim for higher computing power and quantum supremacy.

"Jiuzhang 2.0," which has 113 detected photons, and the "Zuchongzhi 2.1" 66-qubit programmable superconducting quantum computing systems developed by Chinese scientists in 2021, have made China the only country to achieve a quantum computational advantage through two mainstream technical routes: one via photonics quantum computing technology, and the other via superconducting quantum computing technology.

Wang Zhen, deputy general manager of China Telecom Quantum Group, a quantum computing company with investment from China Telecom, said that the company will cooperate with QuantumCTek to develop a quantum computer with the new "Xiaohong" chip, which global users will have access to through a quantum computing cloud platform developed by China Telecom Quantum Group.

"It will allow users in various fields to conduct research on problems and algorithms of practical value efficiently, and accelerate the application of quantum computing in actual scenarios," Wang said.

9.Can We Balance Security and Privacy? Thoughts 10 Years After Snowden

by Matthias Pfau

https://www.forbes.com/sites/forbestechcouncil/2024/04/24/can-we-balance-security-and-privacy-thoughts-10-years-after-snowden/?sh=53baea807b42

More than 10 years have passed since Edward Snowden revealed the worst surveillance scandal of the FBI and the NSA in U.S. history. His revelations sparked a vivid discussion—one that can be looked at with more precision now that the heated debate that started one decade ago has settled: How can we balance the security and privacy requirements of our modern societies?

Snowden brought some of the most intrusive surveillance programs of U.S. authorities to light, the most prominent ones being PRISM, XKeyscore and Boundless Informant. Once the public started to understand how much of their private data they willingly share online is being siphoned off, analyzed and scanned, the question arose whether this form of surveillance is required to keep citizens safe or violate citizens' privacy rights without measurable benefit.

Balancing Security And Privacy—Is It Possible?

The delicate balance between security imperatives and the fundamental right to privacy must be discussed openly by every society. As an expert in encryption and cybersecurity, I am absolutely certain that the Snowden leaks not only exposed the extent of government surveillance but also underscored the urgent need for strong end-to-end encryption to protect the privacy of citizens and businesses alike. At the same time, encryption must not stand in the way of national security, which is what government authorities often claim it would do, but better ways to protect citizens are possible.

First of all, it's essential to note that our internet as it exists today would not be possible without strong end-to-end encryption. We use it every day for online banking, sharing sensitive medical information, messaging or communicating via email. Encryption is the only technical measure we have to protect data online, not just from our own authorities to eavesdrop on it, but also from malicious attackers, economic espionage or state-sponsored surveillance of foreign countries such as China or Russia. Encryption is the very foundation of our modern web and the basis of any cybersecurity strategy.

However, the Snowden disclosures revealed that government agencies used to exploit vulnerabilities in encryption protocols to collect data and even forced American technology companies to provide backdoor access, undermining the very protections meant to safeguard privacy.

Back in 2013, it was a great surprise when it was revealed that tech corporations had collaborated with intelligence agencies in their surveillance activities or submitted to government demands for user data. This raised ethical as well as moral questions about corporate responsibility, user privacy rights and user trust in these corporations. Following the Snowden leaks, an increasingly number of people who were previously ignorant of privacy concerns now understood why privacy matters. They started to look for alternative services that could guarantee privacy by default through employing end-to-end encryption protocols.

Key Lesson From The Snowden Leaks

One of the key lessons learned from the Snowden leaks is that whatever data is out there is vulnerable to surveillance. Intelligence agencies such as the NSA were—and still are—able to collect data on a massive scale, not just the data of foreigners, but also data of American citizens, even though prohibited by the Fourth Amendment. Thus, the erosion of privacy became known with this unbelievable scandal, and for the first time, concerns were rising, and the understanding that our privacy is valuable became commonly agreed upon.

As a consequence, privacy activists, as well as cryptography experts, call to strengthen encryption standards and fortify digital defenses against unsolicited intrusion. However, at the same time, authorities

keep demanding more data from tech companies and politicians try to undermine encryption with legislative approaches, particularly in the Five Eyes countries. Their arguments are that end-to-end encryption impedes law enforcement and intelligence agencies in their efforts to combat terrorism, child sexual abuse, cybercrime and other threats to national security.

Complex Issue

Indeed, the authorities like to present the argument that national security requirements and privacy rights are polar opposite of each other and it would be an immense challenge to balance the two, if possible at all. In their opinion, national security comes first and privacy rights should be sacrificed for that greater goal.

However, as a German, I am very cautious about following this argument. In fact, history teaches us that a loss of privacy can have devastating consequences—not just for the individual but also for the entire society. It can even put national security at risk by undermining democracy and enabling authoritative tendencies to thrive within a community.

While it is true that malicious actors on the Internet can exploit encryption to hide their illegal activities, it is also true that a cooking knife can be used to kill someone. It is clear what I am trying to get at: We can't devalue a technology as crucial as encryption because it is being abused by criminals.

Maintaining strong end-to-end encryption without allowing a backdoor is paramount not just to protecting privacy rights but also to upholding national security. Weakening encryption standards or mandating backdoor access would dangerously expose our digital and physical infrastructure to malicious attackers and state-sponsored hacking.

Security And Privacy Belong Together

In conclusion, regarding the Snowden leaks, there is only one solution to balancing security and privacy requirements: Privacy rights are indisputable. Governments and authorities must (and can) find ways to combat terrorists and other threats to national security with targeted surveillance measures—not by monitoring the entire population of a country.

If we submit to general mass surveillance out of false fears of terrorists, we give up not just our privacy but also our freedom. 100% security is never possible—whether we allow mass surveillance or not. But the best possible security can only be achieved with maximum privacy because the encryption that makes our online life private also protects us from terrorists, such as malicious attackers on the web, as well as state-sponsored surveillance by autocratic countries.

10.Quantum random number generation technology made available to thousands of businesses worldwide

by Equinix
https://www.equinix.co.uk/newsroom/press-releases/2024/04/quantum-random-number-generation-technology-made-available-to-thousands-of-businesses-worldwide

Quside, a quantum technology company, is working closely with Equinix, the world's digital infrastructure company®, to enable easy access to the latest quantum random number generation technologies to help customers build the strongest cryptographic foundation to defend against increasingly sophisticated attacks.

This unusual concept of randomness in cyber security is known as entropy. In cryptography, entropy creates completely unpredictable strings of random numbers, making it exceptionally difficult for bad actors to predict patterns and hack into systems. Entropy, which can only be produced by hardware, is at the foundation of security. If poorly generated, it can lead to completely insecure and vulnerable systems.

Through its globally interconnected Equinix Fabric network, Equinix enables businesses worldwide to connect with this highly innovative and robust cyber security solution on high-speed, low-latency, and private network connections. By allowing seamless communication between quantum entropy systems and operational data processing infrastructure, Equinix and Quside are lowering the barrier to world-class security for thousands of businesses across the globe.

For example, if a financial institution or any other business, based anywhere in the world on Equinix's network, was looking to offer even more protection of data protection to its customers, they could now uplevel their encryption with Quside's quantum technology without changing or investing in any additional hardware – thanks to being part of Equinix's interconnected ecosystem.

Equinix already supports a number of quantum businesses as part of its network of over 10,000 customers worldwide. It is already well placed to support businesses such as Quside on their growth journey and lead the transition towards a range of quantum technologies for multiple sectors, including enhanced cybersecurity options and improved power efficiency.

"Equinix plays a crucial role for customers in facilitating global access to Quside's unique quantum entropy technology". said Carlos Abellan CEO/Co-founder at Quside. "To truly harness the benefits of Quside's entropy solution in their cloud transition, customers require secure, private, and scalable infrastructure. Equinix's IBX data centers offer the perfect scalable solutions that can easily adapt to changing computational demands, allowing our customers to easily connect to and expand their quantum entropy capabilities as needed." He added.

"As businesses seek ever more sophisticated solutions for modern problems, Equinix is proud to support the growth, scale and democratisation of the quantum industry," said Petrina Steele, Global Lead, Emerging Technologies, AI, Quantum & Edge for Equinix. "Working with businesses such as Quside provides our customers with unique access to some of the most innovative security solutions on the planet for the on-going transition to quantum-safe cybersecurity and efficient randomized accelerated computation.

Operating in the heart of Europe's bustling interconnectivity network, Quside focuses on key sectors including government, finance, healthcare, telecommunications, and cloud computing. Quside products deliver highly performant, scalable, quality, and measurable quantum entropy and can be used in conventional, post-quantum, and quantum cryptography systems.

Equinix data centers provide the essential infrastructure, security, and connectivity required to support the development and deployment of quantum cryptography and entropy generation systems, enabling organisations to leverage the power of quantum technologies for enhanced cybersecurity and data protection.

11.Tohoku University-Led Research Team Achieves Room-Temperature Quantum-Metric Manipulation

by Matt Swayne
https://thequantuminsider.com/2024/04/23/tohoku-university-led-research-team-achieves-room-temperature-quantum-metric-manipulation/

Researchers manipulated a fundamental but often overlooked quantum property — known as the quantum-metric structure — at room temperature, according to a study published in Nature. The Tohoku University-led team of researchers, who suggest the discovery has implications for quantum computing, used a topological chiral anti-ferromagnet, Mn3Sn, which features a highly tunable chiral-spin structure.

The researchers showed how the quantum-metric structure in Mn3Sn can be altered among various states using moderate magnetic fields or through interfacial engineering of spin textures with spin–orbit interactions. The research highlights the feasibility of using these properties at room temperature, which would increase the practical applications of quantum-metric effects in quantum devices.

Quantum-metric properties belong to the geometric characteristics of Bloch electrons, which are influenced by quantum mechanics within a crystal lattice. This new method of manipulation at room temperature effectively overcomes challenges seen in previous studies, such as those involving the material MnBi2Te4, where quantum-metric effects were lost around 25 degrees Kelvin and required much stronger magnetic fields to modify states.

This finding may be critical in quantum computing operations because it addresses the essential challenge of balancing robustness with controllability in quantum-metric structures. The use of topological chiral antiferromagnets like Mn3Sn not only boosts the stability of these quantum properties but also provides a straightforward approach for their precise control through external adjustments.

The practical applications arising from this study are substantial. For example, encoding information within the quantum-metric structure of a material could lead to the development of topologically protected memory devices, offering enhanced stability and reduced susceptibility to external disruptions, which are typical challenges in quantum computing applications.

Additionally, the research points toward potential innovations in signal processing. The observed second-order nonlinear current effects in Mn3Sn could transform input signals into their square, indicating uses in signal rectification and noise sensors. These sensors could be instrumental for probing the topological structures of Bloch states and for monitoring time-dependent electrical fluctuations, crucial for advancing quantum computing technologies.

The manipulation mechanism through internal spin–orbit interactions, compatible with general magnetic materials, also expands the range of materials that can exhibit these quantum-metric effects. This broadening of material candidates not only promotes further research in the field but also enhances the integration of these materials into existing technologies.

12.Decrypting the Future: Programmable Cryptography and its Role in Modern Tech

by Felix Xu
https://thequantuminsider.com/2024/04/23/guest-post-decrypting-the-future-programmable-cryptography-and-its-role-in-modern-tech/

As cryptographic technologies continue to advance and create new uses in our lives, the processes they carry out become increasingly complex. While a tremendous amount can be done with simple cryptographic primitives, it is what they can achieve when combined that is the most exciting.

Even more impressive is the idea that some cryptographic protocols are designed with hardware description capabilities, granting them the power to tackle universal challenges. This idea, fittingly called "programmable cryptography," has the promise of making more complicated actions possible by, to paraphrase Brian Gu, turning the mathematical problem of designing new protocols into the programming problem of combining existing ones.

To determine how programmable cryptography can be most useful in our daily lives, we need to first understand the different layers of cryptographic application from high-level goals to low-level algorithms. Below are three considerations for doing this.

Understanding The Basics – Programmable Cryptography's Simple Cipher Origin

As the reliance on data in our daily lives grows, new and improved methods of safeguarding it are continuously needed. It is truly staggering to think of how much information is processed online these days. More immediate to most people is how much more time they spend interacting with data now than they did even a few years ago. All of this information they produce, engage with, review, and send is at risk of being spied on, stolen, or manipulated if it is not properly protected.

This is why there is always a need for cryptography. This is why new and improved methods of keeping data private continue to be developed.

Like many other disciplines, cryptography is based on simple concepts that are scaled up as the task becomes more interesting. These concepts, referred to as "cryptographic primitives," are often basic but can be combined to build something complex.

For example, consider one of the oldest codes, the Cesar cipher. Named after its most famous user, it involves writing words in a cipher text that shifts three letters back from the original message. In this case, the word "the" would be written "qeb." Each letter is shifted to the one that is three spots ahead of it in the English alphabet.

This code may be simple, but it is well-tested. While it is not the most secure method in the world, it can be combined with other techniques to make it stronger.

To take another example, the Vigenère cipher is a tool for encoding a message using several different Cesar ciphers. In this system, each message is combined with a key that indicates how many places to shift the letters in the message, but each letter has a different number of shifts. The "L" in lemon tells you to shift the first letter in the message twelve spaces, as L is the twelfth letter in the English alphabet. The "E" tells you to shift the second letter to five spaces, and so on.

So, “apple” becomes “peszr.” Without access to the key, it becomes much more difficult to decode the message. However, a brute force calculation can determine what the message is, given enough time. By combining existing tools in a new way, the level of security increases dramatically.

As you can probably guess, it is often much, much easier to combine existing ciphers such as these together in new, more complex ways than it is to invent a new system. Cesar died a long time ago, and we are still using his codebook.

Much of modern cryptographic technology stands on a similar pedestal. Hiring a cryptographer to write new proof is quite time-consuming and is not guaranteed to work. Additionally, cryptographic primitives such as RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), or Digital Signature systems are known to work and can easily be applied to a wide range of problems. For instance, RSA is widely used for secure data transmission, while AES is a standard for encrypting sensitive data. If they are combined, they can provide innovative functionality and solve more complex problems than any of them could do alone.

While combining simple methods together is a great way to make more complex systems, there are limitations to it. Each of these primitives is designed to be good at a particular task, and it is not uncommon that mistakes are made when combining them that leave their weaknesses exposed.

Increasing Privacy with Mid-Level Protocols

Mid-level protocols target more advanced features and functionalities. Homomorphic encryption is a protocol that allows for encrypted data to be processed without having to decrypt it first. Examples of it exist today, though it is still in its early phases – yet, the concept has many obvious possible applications. Consider how often sensitive yet useful data, such as medical records, are stolen from organizations that need access to it to help you. What if it were possible to interact with your encrypted medical information without ever decoding it?

One way to do this is **Multi-Party Computation (MPC)**, a tool for hiding inputs provided by different actors working together on a common output. It is often described as the “Millionaire problem.”

Imagine that there are two millionaires who want to learn which of them has more money without revealing their net worth. Using MPC, they can add their encrypted net worth to a program designed to compare the values and determine which one of them entered a larger value – all while not being able to see either of their inputs.

Zero-Knowledge Proofs (ZKPs) are more well-known due to their ability to allow a *prover* to tell another person, often called the *verifier*, that something is true without saying anything else. Typically, they provide this service to a single user; a person asks for proof, and they get it. There are a number of ZKPs, including zk-SNARK and zk-STARK. Each has its own advantages and disadvantages.

As research on these advanced protocols has progressed, the focus has expanded toward developing general-purpose cryptographic protocols. These initiatives aim to prove that it’s feasible for cryptography to enable universal computation to be done securely and privately. Initially, these endeavors were purely theoretical, prioritizing feasibility over practical implementation efficiency. However, as research has deepened, cryptographers have shifted their attention toward making these concepts practically applicable. They enhance, combine, and invent new protocols and components. Often, the ultimate protocol ends up being a hybrid, leveraging the strengths of multiple approaches. For example, homomorphic encryption utilizes zero-knowledge proofs for range proofs to ensure calculations remain within a valid range. Meanwhile, MPC protocols might incorporate elements of homomorphism for executing non-linear operations.

The Future of Programmable Cryptography

Among the plethora of experimental protocols, some have edged close enough to the practical utility that they are paving the way for real-world development, functioning similarly to compilers by interpreting high-level languages and converting them into circuits that protocols can process. Achieving this compiler-like capability, complete with support for Turing-complete computation, marks the advent of what we call programmable cryptography.

Programmable cryptography is still a new concept, but one that offers the chance to make very complicated problems much simpler without the expense of creating a brand-new system for one application. This possibility alone will likely drive a great deal of interest in the field.

Perhaps the most encouraging aspect of all is that society is still in an early stage of exploring the uses of this technology. ZK proofs were devised in the 1980s, but only made possible in 2012. There may be many possible combinations of mechanisms that nobody has dreamed of yet. The next world-shaking idea could arrive tomorrow. We may not even be able to guess what it will do.

13.A Weakness in One of the NIST PQC Algorithms Was Not Uncovered After All

by GQI
https://quantumcomputingreport.com/a-weakness-in-one-of-the-nist-pqc-algorithms-was-not-uncovered-after-all/

There was a recent flurry of concern over the strength of the Lattice based encryption algorithms approved by NIST due to a paper titled Quantum Algorithms for Lattice Problems published earlier this month by Yilei Chen, a professor at the Tsinghua University Institute for Interdisciplinary Information Science (IIIS). Two algorithms this would possibly have affected include ML-KEM (CRYSTALS-Kyber) and ML-DSA (CRYSTALS-Dilithium) which use an LWE (Learning with Errors) approach. These algorithms are based upon the computationally hard problems of determining the length of the shortest nonzero vector in a given n-dimensional lattice. His paper proposed a method to find a polynomial time algorithm for doing this with a quantum computer. The current best algorithms are only able to do this in exponential time.

Professor Chen did post a 65 page paper describing the algorithm that included nine steps. Immediately, many researchers started reviewing it to see if any errors in it could be found. It turns out there was. A problem was found in Step 9 and the author has admitted he doesn't know how to fix it. The paper is still of interest to researchers, but at this point it no longer represents a threat to the Lattice based cryptographic codes.

However, there are lessons here for anyone responsible for implementing quantum safe cryptography within their organizations. The first is to ensure that your implementation provides a means to maintain crypto agility. Although this research effort no longer threatens the existing codes, we can't say for sure that some brilliant PhD student somewhere will discovery an algorithm that works. There is no mathematical proof available that certifies that the PQC algorithms are bullet proof and there probably never will be. So if someday one of the existing PQC algorithms displays a weakness, an organization should be ready to swap in a alternate algorithm based upon a different approach that isn't threatened. A second lesson is to implement hybrid solutions that use both the traditional as well as the PQC algorithms.

That way if a weakness is found in the PQC algorithm, the adversary would still need to break through the classical algorithm in order to decrypt the message. Apple has taken this approach in the recent update to their iMessage app.

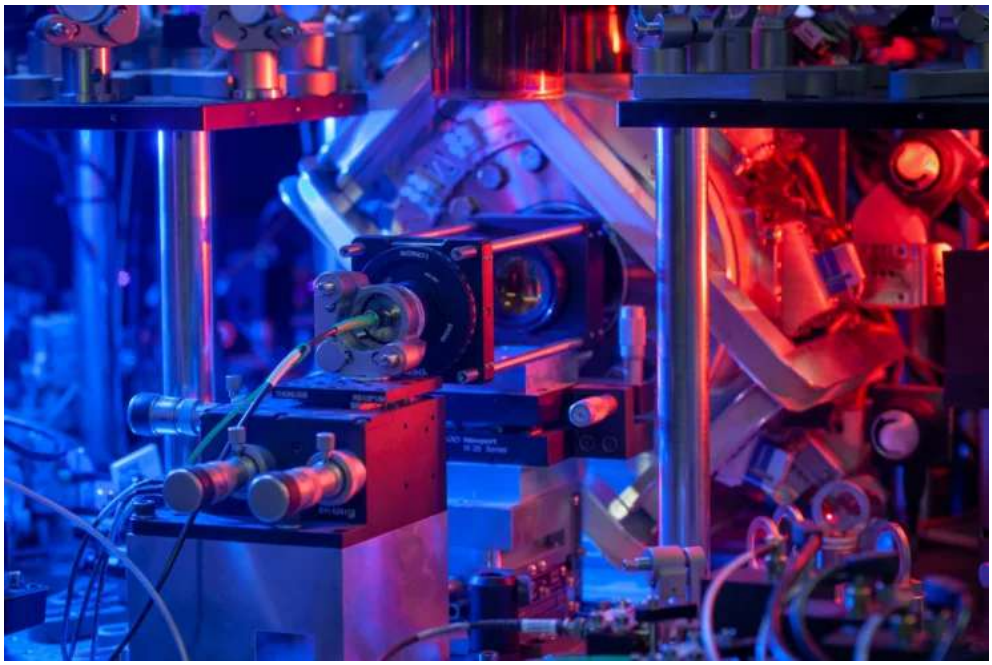
14.Breakthrough in Quantum Cloud Computing Ensures its Security and Privacy

by Fiona Jackson
https://www.techrepublic.com/article/quantum-cloud-computing-security-privacy/

*Oxford University researchers used an approach dubbed "**blind quantum computing**" to connect two quantum computing entities in a way that is completely secure.*

Businesses are one step closer to quantum cloud computing, thanks to a breakthrough made in its security and privacy by scientists at Oxford University.

The researchers used an approach dubbed 'blind quantum computing' to connect two quantum computing entities; this simulates the situation where an employee at home or in an office remotely connects to a quantum server via the cloud. With this method, the quantum server provider does not need to know any details of the computation for it to be carried out, keeping the user's proprietary work secure. The user can also easily verify the authenticity of their result, confirming it is neither erroneous nor corrupted.



Ensuring the security and privacy of quantum computations is one of the most significant roadblocks that has held the powerful technology back so far, so this work could lead to it finally entering the mainstream.

Despite only being tested on a small scale, the researchers say their experiment has the potential to be

scaled up to large quantum computations. Plug-in devices could be developed that safeguard a worker's data while they access quantum cloud computing services.

Professor David Lucas, the co-head of the Oxford University Physics research team, said in a press release: "We have shown for the first time that quantum computing in the cloud can be accessed in a scalable, practical way which will also give people complete security and privacy of data, plus the ability to verify its authenticity."

What is quantum cloud computing?

Classical computers process information as binary bits represented as 1s and 0s, but quantum computers do so using quantum bits, or qubits. Qubits exist as both a 1 and a 0 at the same time, but with a probability of being one or the other that is determined by their quantum state. This property enables quantum computers to tackle certain calculations much faster than classical computers, as they can solve problems simultaneously.

Quantum cloud computing is where quantum resources are provided to users remotely over the internet; this allows anyone to utilise quantum computing without the need for specialised hardware or expertise.

Why is 'blind quantum computing' more secure?

With typical quantum cloud computing, the user must divulge the problem they are trying to solve to the cloud provider; this is because the provider's infrastructure needs to understand the specifics of the problem so it can allocate the appropriate resources and execution parameters. Naturally, in the case of proprietary work, this presents a security concern.

This security risk is minimised with the blind quantum computing method because the user remotely controls the quantum processor of the server themselves during a computation. The information required to keep the data secure — like the input, output and algorithmic details — only needs to be known by the client because the server does not make any decisions with it.

"Never in history have the issues surrounding privacy of data and code been more urgently debated than in the present era of cloud computing and artificial intelligence," said Professor Lucas in the press release.

"As quantum computers become more capable, people will seek to use them with complete security and privacy over networks, and our new results mark a step change in capability in this respect."

How does blind quantum cloud computing work?

Blind quantum cloud computing requires connecting a client computer that can detect photons, or particles of light, to a quantum computing server with a fibre optic cable. The server generates single photons, which are sent through the fibre network and received by the client.

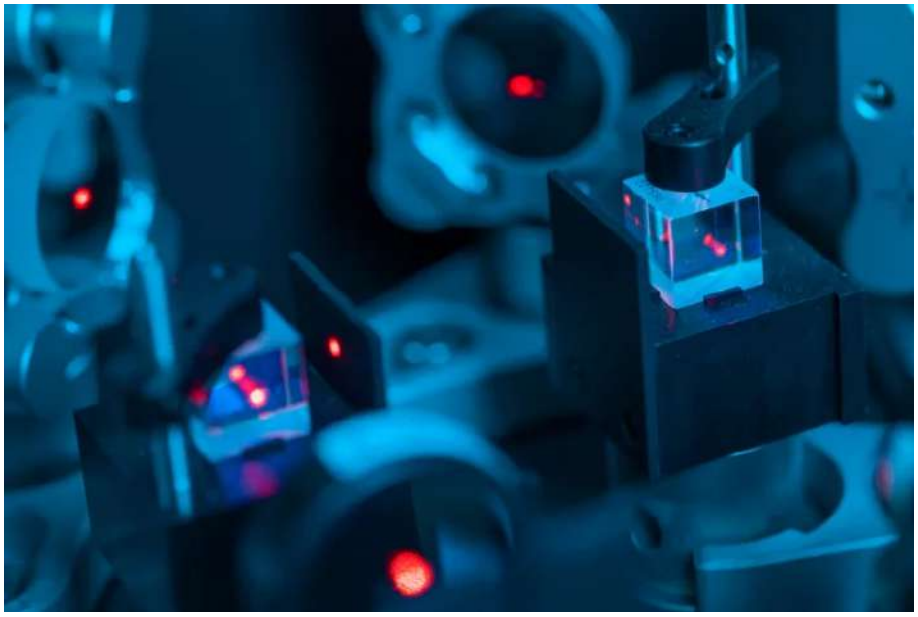
The client then measures the polarisation, or orientation, of the photons, which tells it how to remotely manipulate the server in a way that will produce the desired computation. This can be done without the server needing access to any information about the computation, making it secure.

To provide additional assurance that the results of the computation are not erroneous or have been tampered with, additional tests can be undertaken. While tampering would not harm the security of the data in a blind quantum computation, it could still corrupt the result and leave the client unaware.

"The laws of quantum mechanics don't allow copying of information and any attempt to observe the

state of the memory by the server or an eavesdropper would corrupt the computation," study lead Dr Peter Drmota explained to TechRepublic in an email. "In that case, the user would notice that the server isn't operating faithfully, using a feature called 'verification', and abort using their service if there are any doubts.

"Since the server is 'blind' to the computation — i.e., is not able to distinguish different computations — the client can evaluate the reliability of the server by running simple tests whose results can be easily checked.



"These tests can be interleaved with the actual computation until there is enough evidence that the server is operating correctly and the results of the actual computation can be trusted to be correct. This way, honest errors as well as malicious attempts to tamper with the computation can be detected by the client."

What did the researchers discover through their blind quantum cloud computing experiment?

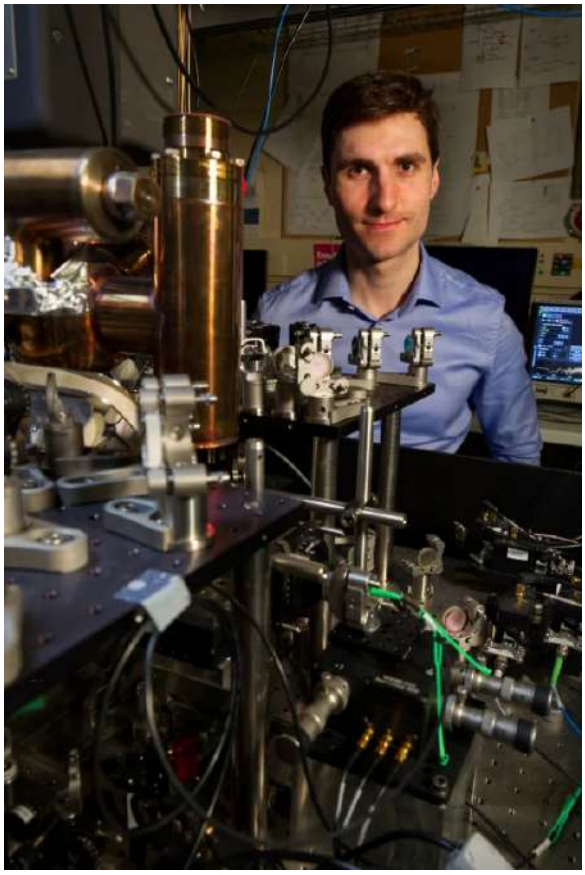
The researchers found the computations their method produced "could be verified robustly and reliably", as per the paper. This means that the client can trust the results have not been tampered with. It is also scalable, as the number of quantum elements being manipulated for performing calculations can be increased "without increasing the number of physical qubits in the server and without modifications to the client hardware," the scientists wrote.

Dr. Drmota said in the press release, "Using blind quantum computing, clients can access remote quantum computers to process confidential data with secret algorithms and even verify the results are correct, without revealing any useful information. Realising this concept is a big step forward in both quantum computing and keeping our information safe online."

The research was funded by the UK Quantum Computing and Simulation Hub — a collaboration of 17 universities supported by commercial and government organisations. It is one of four quantum technology hubs in the UK National Quantum Technologies Programme.

How could quantum computing impact business?

Quantum computing is vastly more powerful than conventional computing, and could revolutionise how we work if it is successfully scaled out of the research phase. Examples include solving supply chain problems, optimising routes and securing communications.



Dr Peter Drmota said that the research is “a big step forward in both quantum computing and keeping our information safe online.”

In February, the U.K. government announced a £45 million ($57 million) investment into quantum computing; the money goes toward finding practical uses for quantum computing and creating a “quantum-enabled economy” by 2033. In March, quantum computing was singled out in the Ministerial Declaration, with G7 countries agreeing to work together to promote the development of quantum technologies and foster collaboration between academia and industry. Just this month, the U.K.’s second commercial quantum computer came online.

Due to the extensive power and refrigeration requirements, very few quantum computers are currently commercially available. However, several leading cloud providers do offer so-called quantum-as-a-service to corporate clients and researchers. Google’s Cirq, for example, is an open source quantum computing platform, while Amazon Braket allows users to test their algorithms on a local quantum simulator. IBM, Microsoft and Alibaba also have quantum-as-a-service offerings.

But before quantum computing can be scaled up and used for business applications, it is imperative to ensure it can be achieved while safeguarding the privacy and security of customer data. This is what the Oxford University researchers hoped to achieve in their new study, published in Physical Review Letters.

Dr. Drmota told TechRepublic in an email: “Strong security guarantees will lower the barrier to using powerful quantum cloud computing services, once available, to speed up the development of new technologies, such as batteries and drugs, and for applications that involve highly confidential data, such as private medical information, intellectual property, and defence. Those applications exist also without added security, but would be less likely to be used as widely.

“Quantum computing has the potential to drastically improve machine learning. This would supercharge the development of better and more adapted artificial intelligence, which we are already seeing impacting businesses across all sectors.

“It is conceivable that quantum computing will have an impact on our lives in the next five to ten years, but it is difficult to forecast the exact nature of the innovations to come. I expect a continuous adaptation process as users start to learn how to use this new tool and how to apply it to their jobs — similar to how AI is slowly becoming more relevant at the mainstream workplace right now.

“Our research is currently driven by quite general assumptions, but as businesses start to explore the potential of quantum computing for them, more specific requirements will emerge and drive research into new directions.”

15.Unbreakable trust: Safeguarding brands with the power of cryptographic signatures

by Padmakumar Nair
https://www.expresscomputer.in/guest-blogs/unbreakable-trust-safeguarding-brands-with-the-power-of-cryptographic-signatures/111313/

In today’s digital landscape, the stakes for brand protection have never been higher. The pervasive threat of counterfeit products and the ever-evolving landscape of online fraud present formidable challenges to maintaining consumer trust. The counterfeit industry, fueled by sophisticated technology and global networks, has become increasingly adept at producing convincing replicas that can deceive even the most vigilant consumers. In this environment, the need for robust brand protection measures has never been more urgent. However, amidst these challenges, there exists a beacon of hope: cryptographic signatures. These cutting-edge tools offer a promising solution to the pressing issue of brand protection, providing a means to establish unshakable trust and safeguard the reputation of brands in ways previously unimaginable.

Technology as the Foundation of Trust

Technology, spanning a spectrum of cryptographic techniques beyond blockchain, serves as the cornerstone for implementing cryptographic signatures in brand protection strategies. These techniques not only ensure data integrity and authenticity but also guarantee confidentiality, laying a robust foundation for trust in digital interactions. By leveraging these technological advancements, brands can forge ahead with confidence, knowing that their digital assets are fortified against the threats of tampering and fraud.

The Power of Cryptographic Signatures

At the heart of cryptographic signatures lies a profound concept: the assurance of authenticity and integrity in digital interactions. Similar to how a handwritten signature uniquely identifies an individual, these signatures serve as digital fingerprints, uniquely binding data or documents to their creators or originators. This process, facilitated by complex mathematical algorithms, generates immutable identifiers that are practically impervious to replication or tampering.

But what makes cryptographic signatures truly remarkable is their ability to ensure the integrity of data. Through rigorous mathematical processes, these signatures create a binding link between the signed data and its originator, rendering any alteration immediately detectable. This robust mechanism serves as a bulwark against tampering and forgery, guaranteeing the authenticity and reliability of digital assets.

Furthermore, such signatures play a pivotal role in authenticating the origin and ownership of digital content. Just as a handwritten signature confirms the identity of its signer, a cryptographic signature verifies the legitimacy of the sender or creator of digital assets. This authentication process not only fosters trust between parties but also provides irrefutable proof of the source's authenticity.

Perhaps one of the most compelling attributes of such signatures is their ability to provide non-repudiation. Once affixed to a document or transaction, a cryptographic signature unequivocally binds the signer to the action, leaving no room for denial or dispute. This attribute enhances the trustworthiness of digital interactions, as parties can rely on the indisputable evidence furnished by such signatures.

In an era marked by rampant digital fraud and sophisticated counterfeiting schemes, these signatures emerge as indispensable allies in the fight for brand protection. Their resilience against tampering, their ability to authenticate origins, and their provision of non-repudiation make them invaluable assets in safeguarding brands' reputations and fostering trust among consumers.

As brands navigate the intricate maze of the digital landscape, cryptographic signatures offer a beacon of reliability and assurance. Their adaptability to various use cases and industries underscores their universal applicability, providing a robust framework for establishing trust in digital ecosystems.

The influence of cryptographic signatures extends far beyond conventional security measures; they epitomise an unwavering dedication to integrity, authenticity, and trust. Embracing these signatures heralds a new era where brands not only defend themselves against fraud but also pioneer a future built on transparency and accountability. By leveraging this technology, brands can fortify their defences, safeguard their reputations, and champion the unwavering trust of consumers in an ever-evolving digital landscape.

16.Local Qubit Control Brings New Capabilities to QuEra's Quantum Computer

by QuEra
https://www.quera.com/press-releases/local-qubit-control-brings-new-capabilities-to-queras-quantum-computer

QuEra Computing, the leader in neutral-atom quantum computers, today announced it is adding local qubit control to its 256-qubit quantum computer - **Aquila** - to further broaden the set of problems that it can address. Also known as local detuning, this capability gives Aquila's users a new degree of flexibility

in programming qubits independently and represents an important next step on the company's path to offering large-scale, fault-tolerant quantum computers. The local detuning capability is now available on Amazon Braket, through which QuEra's quantum computers have been available to the public for over 18 months. The new capability comes alongside two additional enhancements to the already powerful qubit position programmability, enabling more flexibility in user-defined qubit arrangements, and larger system sizes.

"QuEra's progress towards universal, fault-tolerant quantum computers proceeds along two paths: scale and control. QuEra's publicly-available machine Aquila already leads the industry with 256 qubits, and we are now adding a substantial new degree of local qubit control" said Alex Keesling, CEO at QuEra Computing. "This functionality gives users additional levels of programmability not yet offered in other comparable devices. We are continuing to innovate with our analog quantum capabilities while developing the digital gate-based systems that we announced earlier this year.

Quantum computers with analog capabilities, such as QuEra's Aquila, are effective at solving machine learning, optimization, simulation problems, and other similar types of computations. Adding new degrees of programmability to the system's qubits and extending the range of the already available qubit position programmability, now provides users key advantages for computing a wider class of problems in each of these categories.

First, controlling individual qubits locally means that their starting states can be individually altered, as opposed to the global control methods previously available. Commonly known as 'state preparation,' beginning operations with qubits in multiple starting states allows computing on a much broader range of input data. For studying dynamical phenomena in physics using quantum simulation approaches, this capability enables stating the dynamics in a range of non-trivial, non-equilibrium states.

Second, by encoding input data into the pattern of analog detuning magnitudes applied to different qubits, Aquila can operate on more general classical data, opening the door to more powerful machine-learning workflows and many other real-world applications. This innovation allows for the encoding of both classification and prediction machine learning problems, as well as optimization problems, directly onto the hardware. This drastically simplifies the implementation of many classes of problems on the quantum computer, including a wider range of optimization problems and even enabling generative machine learning functionality.

The comprehensive new capability of local qubit programmability will deliver measurable and tangible value across multiple industries. For example, in the pharmaceutical sector, modeling how proteins fold or how molecules bind can now be mapped into an optimization problem and encoded directly on Aquila using local detuning. This could become an important tool for computer-aided drug discovery, and could even assist in later stages of the drug development process, such as reducing the costs of clinical trials and increasing the success rate of regulatory approvals.

"The enhanced position programmability is indeed crucial to expanding Aquila's capabilities for quantum simulations," said Arnab Banerjee, Assistant Professor of Physics and Astronomy at Purdue University. "Recently, we tested this new capability and were able to sort new complex geometries for a project that probes new quantum phases, and we are very excited about the successful results

"As early users of the upgraded Aquila device, we're thrilled with its new features that have enabled initial experiments on string breaking, showcasing the sophisticated potential of quantum simulations within lattice gauge theories," said Peter Zoller, Professor of Theoretical Physics, University of Innsbruck.

17.D-Wave Introduces New Fast Anneal Feature, Extending Quantum Computing Performance Gains

https://www.dwavesys.com/company/newsroom/press-release/d-wave-introduces-new-fast-anneal-feature-extending-quantum-computing-performance-gains/

A D-Wave Quantum Inc. a leader in quantum computing systems, software, and services and the world's first commercial supplier of quantum computers, today launched the fast-anneal feature, available on all of D-Wave's quantum processing units (QPUs) in the Leap™ real-time quantum cloud service.

The fast-anneal feature has been a key part of D-Wave's research milestones, including work published in Nature Physics (2022) and Nature (2023), demonstrating the advantages of annealing quantum computing over classical algorithms for solving complex optimization problems. With this feature now widely accessible, users can perform quantum computations at unprecedented speeds, greatly reducing the impact of external disturbances such as thermal fluctuations and noise that often hinder quantum calculations. By offering extended control for notably faster annealing times than previously available, the feature paves the way for customers to reproduce and build on D-Wave's landmark optimization results using full-scale coherent annealing quantum computing available through D-Wave's Advantage™ systems and the Advantage2™ prototype, the company's most performant system to date.

"Providing direct access to Fast Anneal, which has been at the heart of D-Wave's recent advancements, represents a significant step forward in our mission to provide customers with the resources they need to drive innovation and achieve extraordinary results," said Dr. Alan Baratz, CEO of D-Wave. "We believe it will further empower them to build industry-shaping applications with the most powerful quantum computing environment available today."

Growing customer demand for D-Wave's latest annealing quantum computing technology is clear from the usage of the two next-generation Advantage2 experimental prototypes, which together have solved nearly eight million customer problems since they were made available in 2022 and 2024.

The fast-anneal feature is anticipated to draw attention from commercial and academic researchers eager to build world-class applications, expand benchmarking studies, and connect increased coherence to better performance.

"The ability to use the fast-anneal feature to directly interact with D-Wave's Advantage2 prototype is particularly exciting for our work building quantum-enhanced generative AI models trained on molecular data to accelerate drug discovery and design new materials," said Christopher Savoie, co-founder and CEO of Zapata AI. "The fast-anneal feature can produce coherent distributions that have the potential to allow more efficient encoding of complex data patterns in a way that is classically impractical. In addition to molecular discovery applications, this feature could also be valuable in other industrial applications involving complex data patterns, particularly in combinatorial optimization problems found across industries."

"By providing direct access to quantum computing's central nervous system, D-Wave is single-handedly opening new horizons for our research on quantum computing and AI," said Ed Heinbockel, president and CEO of SavantX. "We believe the new capability will help us realize significant benefits of coherence on application development that we'd otherwise be unable to achieve."

"Fast Anneal will assist researchers in observing the distinctive physical processes inherent in the quantum world. Heightened coherence and reduced environmental interference, will open avenues in quantum sciences," said Alejandro Lopez-Bezanilla with Los Alamos National Laboratory. "By equipping scientists with technology capable of exploring the interactions of quantum objects with control and minimal disturbances, we anticipate a new era of experimentation free from the limitations that have hindered traditional experimental approaches. With increased quantum coherence, we can finally achieve precise observations of quantum phenomena, previously only accessible in theory but now within reach of experimental validation."

18.Prepping For Post-Quantum Cryptography

by Rahul Rao
https://spectrum.ieee.org/post-quantum-cryptography-2667758178

Encryption today is typically a game of very large numbers. Some of today's cryptographic systems, like RSA or elliptic-curve cryptography, utilize as keys integers that are hundreds or thousands of bits long. Cracking a key requires breaking down one of these integers into its prime-number factors. Even the mightiest non-quantum computers struggle to perform this calculation in any reasonable timeframe.

That is why quantum hardware can completely rewrite the rules of encryption. Quantum computers have a potential weapon called Shor's algorithm that can factorize colossal integers in a dramatically accelerated time.

Fortunately for some, quantum computers aren't yet powerful enough to wield Shor's algorithm on demand. There is still time to introduce alternative security methods like lattice cryptography that are invulnerable to this kind of quantum cracking. For example, the U.S. National Security Agency (NSA) has laid out a plan to switch the country's cloud services, network infrastructure, and more to lattice cryptography algorithms developed by the National Institute for Standards and Technology (NIST).

IEEE Spectrum spoke to Scott Best, a senior engineer at chip design company Rambus, on what needs to happen to transition cryptographic protocols to a world where quantum computers are now longer in the future.

Quantum computers aren't powerful enough just yet. How urgent, then, is it to switch everything to a quantum-resistant protocol like lattice cryptography?

Scott Best: Commercially, it's not essential right now. That is only because [smartphones and other cloud-touching consumer electronics] don't have a terrifically long lifetime in the field. They have a lifetime around two to five years, and it's not expected that any sort of cryptographically relevant quantum computer is going to be available until 2030 or 2033.

Something with 400 logical qubits that can actually complete Shor's algorithm, which can be used to factor RSA or elliptic curve — that kind of computer is not going to exist for another eight years, let's say. So, any sort of commercial system that's being deployed now can be upgraded in that timeframe.

What sort of applications will transition first or are already transitioning?

Best: There's a lot of interest in saying networking infrastructure absolutely needs to be upgraded as soon as possible.

Defense-facing systems, the stuff that I work on—those don't have a two-to-five-year timeframe in the field, they have a ten-year timeframe in the field. Those absolutely need to be upgraded now, because they are going to still be in service and in operation in that future where cryptographically relevant quantum computers exist.

Automotive is another leading edge, because cars last long enough that they're going to cross into that horizon.

And everyone else follows?

Best: It is a very heavy lift. You really do have to update everything that touches the public cloud and update the protocols. Anything that consumes firmware is going to have to be updated in the future.

That sounds like quite a lot of devices.

Best: I describe it as a very heavy lift, and that's really an understatement. There are billions of devices that connect to the cloud. I think my toaster has firmware upgrades occasionally. It's everywhere, and every single one of those devices could be potentially compromised in a future where RSA and elliptic-curve can be factored.

The NSA wants this transition done by 2033. How fixed is that date?

Best: They want critical networking infrastructure, I think, to be fully on the way to transitioning by 2025. So, all the major cloud vendors…the NSA is pressing them to get things done right now.

And will people and companies listen?

Best: Domestically [in the US], it is the standard. It is considered, at least in the community of people that I speak with, as the equivalent of when an executive order is published out of the White House. This is critically important to domestic internet infrastructure, municipal fire and safety, and security.

It seems like there's a plan, then.

Best: We know currently what the solution is, but the upgrading of all of that is what is going to take us an entire generation. It's going to take a decade to get all of that infrastructure updated to use the new protocol.

What you're racing against is physics. You're trying to solve the problem of the decoherence of logical qubits—[today] they've got 100 or 120 or 140 functional, logical qubits that could be used. Once that number scales up into the 400s, that's when a national lab, a state-funded actor could absolutely just start maliciously breaking digital signature and secure socket technology.

So you're sort of in a race: on one side, just grindstone work of upgrading the entire world's cloud-based infrastructure; on the other hand, it's a race against physics.

Ten years is a long time—could quantum-resistant protocols get cracked before then?

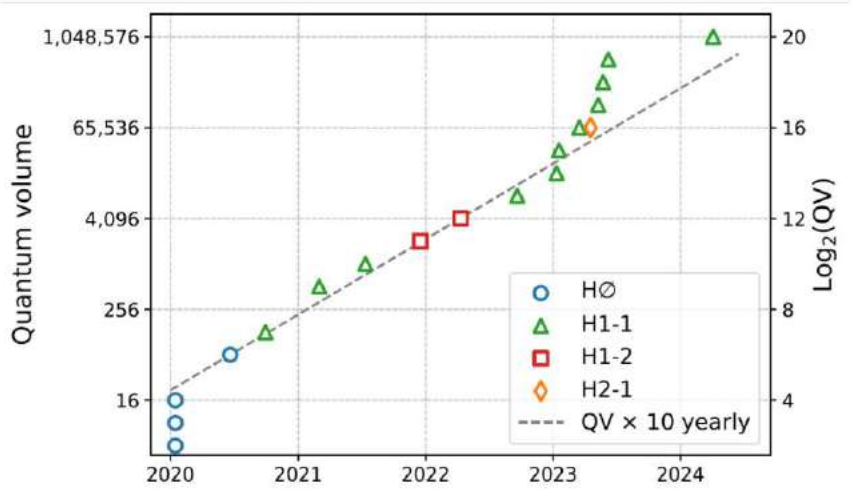
Best: Nobody looks at lattice and says, "you know, there's a gap in the math there." If there is a shortcut, it's a math we haven't invented yet. And that gives a lot of people a lot of confidence that the type of asymmetric cryptography problems that you're trying to solve with this new cryptography have no obvious shortcuts to them.

19.Quantinuum Sets New Records for Both Gate Fidelity and Quantum Volume

by GQI
https://quantumcomputingreport.com/quantinuum-sets-new-records-for-both-gate-fidelity-and-quantum-volume/

Quantinuum has always had a strategy of providing users with qubits that demonstrated the highest possible measure of qubit quality, as measured by both gate fidelity metrics as well as the Quantum Volume measure originally proposed by IBM. In fact, in 2020, they declared a goal of continuing to improve the Quantum Volume measure of their machines by a factor of 10X each year. And to their credit, they have continued to meet or beat this goal every year.

Now, they have reached a new level of qubit quality performance on their 20 qubit H1-1 processor and achieved a two-qubit gate fidelity measure of 99.914% and a Quantum Volume measurement of 1,048,576 (or 2^{20}). The Quantum Volume benchmark was achieved with a circuit that used 20 qubits successfully running a randomized circuit that is 20 layers deep. Although the circuit used in a Quantum Volume test would not be useful for a commercial application, the advantage of this benchmark is that it is hard to "game" to unfairly show better results. We should also point out that this same machine is also in daily use serving end users. So it is not a special machine developed by engineering just to be used for these tests.



We should note that the company has maxed out the capability of the H1-1 processor, since that machine only contains 20 qubits. Another impressive result of Quantinuum's test is that they achieved very

high consistency in performance amongst all the qubits. In other quantum hardware implementations there can be a wide range of qubit quality performance with some qubits being good and other being not-so-good. In this latest test, every qubit pair on this H machine achieved a 99.9%+ two qubit gate fidelity.
The engineers at Quantinuum achieved this result by implementing various improvements in the laser and optics systems inside the machine. The original H1 processor was introduced in October 2020 with 10 qubits and a Quantum Volume level of 128 (or 2^7). And the company has been implementing many incremental upgrades over the years to both improve qubit quality and double the number of qubits.

The next step in their development will be to take all the improvements and learnings from the H1 and apply them to the next generation H2 processor. Currently the H2 supports 32 qubits but the company intends on expanding this in the future as well as improving the qubit fidelity metrics to levels similar to what they have achieved with the H1.

This demonstration is one more step towards reaching a Quantum Advantage level that can provide commercial benefit. Although many people are investigating error correction techniques, we should point out that error correction becomes increasingly more effective and efficient as the raw physical qubit fidelities improve. Although there is still disagreement amongst quantum researchers on whether commercial useful applications will be able to run on uncorrected NISQ level machine, the chances of this occurring also become higher as the raw qubit fidelities improve. So this development will be helpful for use in both non error corrected NISQ implementation as well as more efficient error correction implementations in fault tolerant machines.

We can't describe this development as reaching a Sputnik moment, but it is another forward step in the long path of providing high quality quantum computation and it is synergistic with Quantinuum and Microsoft's research results last month of demonstrating error correction circuits on their processors. For more information about this result, you can view a news release available on the Quantinuum website here. Also, for those who want to dig into the technical details, Quantinuum has posted the technical data of their Quantum Volume test on GitHub here and also posted on GitHub the hardware specifications here.

20.Qunnect Achieves Record-Breaking Performance for Distributing Polarization Qubits on GothamQ Network in NYC

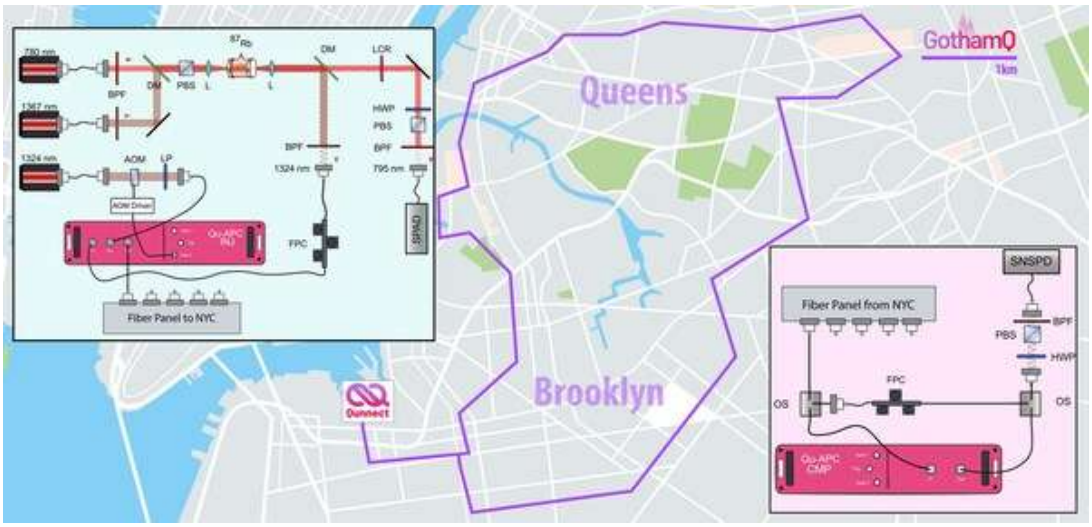
by Qunnect
https://www.prnewswire.com/news-releases/qunnect-achieves-record-breaking-performance-for-distributing-polarization-qubits-on-gothamq-network-in-nyc-302116594.html

Qunnect, a leader in quantum-secure networking technology, today announced that GothamQ, its quantum network utilizing existing commercial fiber optic cable, surpassed previous performance metrics in enabling the distribution of polarization-based quantum entanglement while delivering exceptionally high rates of preservation and fidelity. This technical achievement signifies the viability of Qunnect's quantum networking components to perform entanglement-based protocols over prolonged durations in real-world environments.

``GothamQ's performance as a stable, automated network that can support high-quality entanglement

distribution networking protocols represents a major step forward in unlocking future applications like distributed quantum sensing and computing," said Noel Goddard, CEO of Qunnect. "As we celebrate World Quantum Day, we are proud to showcase Qunnect's first-in-class hardware as an example of the progress made in turning experimental innovations into commercial products."

Unlike most quantum networks, Qunnect uses atoms at room temperature to generate polarization entangled photons, since these qubits are native to other quantum devices such as sensors and computers. By constructing a stable network to distribute polarization qubits, Qunnect has demonstrated a path forward for other quantum networks to host applications beyond secure communications.



For this demonstration, the Qunnect team used its hardware instruments to generate, distribute, and preserve entangled photons over 34 kilometers of fiber within the GothamQ network. Its QU-SRC maintained generation rates between one to ten million polarization-entangled photon pairs per second. Meanwhile, the QU-APC preserved the fidelity of the transmitted photons through an automated protocol, minimizing the quantum bit error rate. The result was a record-breaking 99.84% network uptime over 15 days of continuous operation. During that time, the team:

- Distributed and preserved 500,000 polarization-entangled pairs per second in commercial-grade fiber channels with 17dB of transmission loss
- Maintained a quantum bit error rate below 2.5%

The full test results are published in a manuscript posted on ArXiv today, in celebration of World Quantum Day 2024.

Unlike traditional quantum networks, Qunnect chose to encode quantum bits of information with light polarization for this test, since polarization qubits are native to other quantum devices such as quantum sensors and computers. By constructing a stable network to distribute polarization qubits, Qunnect has demonstrated a path forward for other quantum networks to host applications beyond secure communications.

``This work demonstrates that the field of entanglement distribution networking is ready to transition from proof-of-concept experiments to the era of reliable, 24/7 operation." Said Mehdi Namazi. "Important to note, we used polarization qubits, which are highly practical for transactions at the end nodes, yet notoriously hard to preserve in long, deployed fiber optic channels."

As part of its mission to transform traditional telecom infrastructure into quantum networks, Qunnect's products are all housed in standard server racks. They are currently installed and operating on testbeds around the world. Later this year, Qunnect plans to release the industry's first full-rack quantum networking system to enable users to replicate the entanglement distribution protocols demonstrated in this announcement.

21.World Quantum Day — Putting The 'World' Back In World Quantum Day

by Matt Swayne
https://thequantuminsider.com/2024/04/14/world-quantum-day-putting-the-world-back-in-world-quantum-day/?utm_source=newsletter&utm_medium=email&utm_term=2024-04-14&utm_campaign=Happy+World+Quantum+Day+

As a writer for The Quantum Insider, I report a lot on local quantum ecosystems, regional quantum ecosystems, state quantum ecosystems, national — and on and on.

Don't get me wrong, those communities and those projects to build local quantum communities are vital. Without these initiatives and organizations, the transformative power of quantum technologies would likely remain untapped, particularly as we are in this nascent stage of developing quantum. But creating a strong global quantum ecosystem will not diminish local quantum ecosystems — in fact, a tide to build a world quantum community will lift all local boats.

So, let's take some time World Quantum Day to consider the power and pure potential of the worldwide quantum ecosystem—and consider ways we can merge these local initiatives to reinforce this rapidly growing, quickly maturing global community that can deliver the benefits of quantum technologies to science and society.

We don't have to stretch our imaginations that much because world quantum is a reality right now. But it might be important to consider the power of global research collaborations — and just how limitless this potential is. Here are just a few international collaborations in various aspects of quantum science based on a random jaunt through Google Scholar:

Evidence for Chiral Graviton Modes in Fractional Quantum Hall Liquids

This study explores a fascinating aspect of quantum physics known as chiral graviton modes (CGMs) within a unique state of matter called fractional quantum Hall (FQH) states. Researchers have now, for the first time, detected these elusive CGMs by observing specific vibrations or waves among electrons when they shine circularly polarized light (light that spirals as it moves) on an ultra-cold electronic system. They found that these vibrations have a preferred direction of swirl (chirality) that changes with the density of electrons. This discovery is a big deal because it confirms a key theoretical prediction about the quantum behavior of electrons in FQH states and helps us understand how quantum geometrical properties influence the behavior of electrons in these exotic systems.

Researchers include scientists from China, US and Germany. Read the full paper

Progress on Superconducting Materials

This study, which includes researchers from the US and Germany, focuses on advancements in superconducting materials for Superconducting Radio Frequency (SRF) applications, crucial for both accelerator physics and quantum information science. It showcases the collaborative effort among an international group of researchers working to optimize niobium (Nb) materials to enhance the efficiency and performance of SRF cavities. Read the full paper

Realization of a Fault-Tolerant Quantum Algorithm on a Superconducting Quantum Processor

The study, published in the journal Nature, describes an international collaboration between researchers from the United States, Japan, and Germany who demonstrated the implementation of a fault-tolerant quantum algorithm on a superconducting quantum processor. This represents an important milestone in the development of practical quantum computing. Read the full paper

Room-Temperature Quantum Coherence and Entanglement in Two-Dimensional Materials

This study was published in “Nature Materials”. This study involved researchers from several institutions across multiple countries, including the United States, South Korea, and Germany. The collaboration brought together experts from Stanford University, the Korea Advanced Institute of Science and Technology (KAIST), and the Technical University of Munich, among others

Spin-2 Partner in Particle Collisions

This research explores the production of a new particle suspected to be the spin-2 partner of another quantum entity during particle collisions. It delves into the quantum numbers and potential decay channels of this novel structure, marking a significant leap in quantum physics research. There is a good chance that without international work like this our comprehension of the quantum realm would be greatly diminished.

The team of researchers include scientists from China, Spain, Germany, Slovenia and Portugal. Read the full paper

In fact, while not a majority of research produced, these global collaborations represent a sizable portion — possibly almost a quarter — of total research partnerships. The National Science Foundation (NSF) reports, for example, that the percentage of science and engineering articles produced with international collaboration increased from 18% to 23% from 2010 to 2020. In quantum science, it might even be higher.

We know one reason that scientists engage in international partnerships — they’re successful.

Global collaborations are also deeply etched in the fabric of the scientific enterprise — we encourage our graduate, doctoral and post-doctoral students to travel to other institutions. This tradition is hundreds of years old and likely was prompted by a desire for knowledge disseminations. That dissemination of brain power still works today — even with all the remote opportunities for learning and knowledge gathering.

But, for quantum science, there may be another reason: global research is absolutely necessary. A relatively small number of scientists are engaged in quantum research — and they are spread all over the world. In other words, the **global quantum** aspect of t**he global quantum workforce** is a redundant

term.

This World Quantum Day, let's temporarily put aside ideas of quantum valleys and quantum alleys, quantum highways and quantum islands, and think about how we can intelligently unite friendly nations to build a global quantum ecosystem that amplifies the power of all these quantum ecosystems while we strengthen our resolve to manage the power of quantum responsibly and decrease the timeline of when the potential of quantum is delivered to society.

Here are a few ideas we've come up with — but it's certainly not an exhaustive list.

GENEROSITY WITH TALENT AND KNOWLEDGE

- **Exchange Programs:** Encourage talent exchange programs between institutions, companies and research groups globally. These can include internships, visiting researcher positions and sabbaticals.

- **Open-Source Contributions:** Participate in and contribute to open-source quantum computing projects. This not only helps with the advancement of the field but also puts local talent on the global map. Quantum Open Source Foundation has a great list and the Unitary Fund is a great place for more news and information.

GLOBAL NETWORKING AND PARTNERSHIPS

- **Ecosystem Connectors**: Local, regional and national ecosystems should find ways to connect to each other within their own spheres — while linking with the broader local, regional and national ecosystems across the world.

- **Attend and Host International Conferences:** Attend international quantum technology conferences, workshops, meet-and-greets and symposiums. Hosting such events can also attract global attention to local ecosystems.

- **Network Remotely:** Busy startups can't always be jetting across the world, but remote networking sessions can fill an important gap between complete isolation and international conferences.

- **Strategic Alliances:** Form strategic alliances with leading institutions, labs and companies around the world to collaborate on research, development, and educational initiatives.

IDEA AND RESOURCE SHARING

- **Collaborative Research Projects:** Always be on the lookout for collaborative research projects that bring together researchers from different parts of the world to work on our common goals.

- **Knowledge Repositories:** Create and contribute to global knowledge repositories, including preprint servers and open-access journals focused on quantum technology.

PROMOTING 'COLLABETITION' (THAT'S COLLABORATION AND COMPETITION MERGED TOGETHER, IN CASE THAT LOOKS STRANGE)

- **Joint Ventures:** Encourage joint ventures that pool resources, knowledge and networks from competitors to tackle large-scale quantum projects. You may be surprised just how much your so-called competitors are actually collaborators.

- **Shared Challenges and Competitions:** Participate in and sponsor global quantum challenges and hackathons, which can foster a spirit of collaborative competition. The Airbus and BMW Quantum Computing Challenge 2024 and X Prize are just two examples.

EDUCATION AND OUTREACH

- **Global Quantum Education Platforms:** Develop and contribute to online education platforms that offer courses, seminars, and webinars on quantum technology to a global audience.

- **Public-Private Partnerships:** Engage in public-private partnerships that leverage government, academic, and industry resources to promote quantum technology development on a global scale.

POLICY AND STANDARDIZATION EFFORTS

- **Adopting Technical Standards:** In technological communities, it's not good fences that make good neighbors; it's good standards that make good neighbors. Standards are something the entire global quantum community should advocate.

- **Engage in Policy Advocacy:** Work towards global standards and policies that facilitate the free exchange of quantum research and technologies.

- **Ethical Frameworks:** Contribute to the development of ethical frameworks for quantum technology research and application, ensuring responsible global development.

INVESTMENT AND FUNDING

- **Global Investment Funds:** Participate in or establish investment funds focused on supporting quantum technology startups and projects worldwide.

- **Crowdfunding-Crowdinvesting Platforms:** Here's an idea that might be a bit out-there. But crowdfunding and crowdinvesting platforms are seeing great success in other industries and fields. Utilize crowdfunding platforms to support quantum projects with global impact, engaging the wider community in funding initiatives.

22.Quantum Xchange Joins Migration to Post-Quantum Cryptography Project Consortium

by Matt Swayne
https://thequantuminsider.com/2024/04/12/quantum-xchange-joins-migration-to-post-quantum-cryptography-project-consortium/

Quantum Xchange, delivering the future of encryption with holistic cryptographic agility, visibility, and management solutions, announced that it is collaborating with the National Cybersecurity Center of Excellence (NCCoE) as part of the Migration to Post-Quantum Cryptography Project Consortium. This move is designed to bring awareness to the issues involved in migrating to the National Institute for

Standards and Technology (NIST's) post-quantum cryptography (PQC) and to develop practices to ease replacing current public-key algorithms with NIST-standardized post-quantum algorithms.

Currently, governments and organizations do not have access to a universally acceptable way to guide existing cryptographic standards, guidelines, regulations, or technologies to meet the requirements of migrating to quantum-resistant cryptography. Implementation of quantum-safe algorithms requires identifying hardware and software modules, libraries, and embedded code currently used in an enterprise to support cryptographic key establishment and management underlying the security of cryptographically protected information and access management processes, as well as provide the source and content integrity of data at rest, in transit, and in use.

"Public-key cryptography is widely used to protect today's digital information. With the advent of quantum computing and its potential to compromise many of the current cryptographic algorithms, organizations must begin to plan for many of the technological and operational challenges that migration to post-quantum cryptography will present. This project aims to help organizations to achieve exactly this," said William Newhouse, Security Engineer at NIST NCCoE.

Initially, the project will focus on demonstrating the discovery tools that can provide automation assistance in identifying where and how public-key cryptography is used in various technologies – specifically those employed in data centers, on-premises, or in the cloud and distributed compute, storage, and network infrastructures.

"Being named an official collaborator on the project validates Quantum Xchange's vision statement: Partners in Preserving Our Digital World," said Holly Neiweem, CFOO of Quantum Xchange. "We are committed to sharing our knowledge and bringing to market products and services to inventory the use of cryptography throughout the enterprise, mitigate cyber risk, and ease the transition to quantum-safe cryptography."

This quantum-safe cryptography discovery project will demonstrate tools for discovering quantum-vulnerable cryptographic code or dependencies on such code for several implementation scenarios. In today's digitally-driven environment, it's critical to plan how technologies still reliant on public-key algorithms will be replaced to ensure information is safeguarded.

It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that the information is protected from future attacks.

23.MEPs call for 'urgent action' to implement post-quantum encryption standards

by Martijn Boerkamp
https://physicsworld.com/a/meps-call-for-urgent-action-to-implement-post-quantum-encryption-standards/

Twenty members of the European Parliament have called for urgent action to develop a new standard for data encryption that would protect against quantum computers being used for malicious purposes. In their letter, the members urge the European Commission to develop security measures and regulations to ward off the threat of quantum computers for cybercrime and data breaches.

Quantum computers, once fully developed, have the potential to calculate complex processes that can-

not be easily carried out by classical devices. There is, however, a real threat that they may also be used to hack encrypted information, even present-day information that is currently considered unhackable.

Experts estimate that the commonly used RSA-2048 keys can be cracked by a quantum computer within 24 hours. This puts secret information, for example held by governments or companies, at risk of being stolen.

Even though practical quantum computers still need years, if not decades, to become practical, the complexity of any new encryption standard could take a similar amount of time to implement. Transitioning to a new cryptographic standard to incorporate a wide range of technological domains, such as internet servers, banking and internet-of-things devices, has already started.

The National Institute of Standards and Technology (NIST) in the US has determined the algorithms that will be included as post-quantum encryption standards and these are currently being developed by collaborations around the world. The new standards will be applied to public-key encryption and for digital signatures.

In their letter, the MEPs urge the European Commission to create an inventory of current encryption algorithms that are used by organisations. They want a review of which new (classical) cryptographic libraries can be easily included in current infrastructure and are keen to ensure that hybrid – classical as well as post-quantum cryptographic – encryption is deployed where possible. The MEPs also want a phased implementation to begin as soon as NIST has adopted relevant standards.

“The [relevant] commissions should play an important role in spurring this transition now, by explaining in joint guidance what taking ‘appropriate’ security measures under the different regulatory regimes means, in the view of the development of quantum computers,” the letter states.

24.Post-Quantum Cryptography Gets Performance Testing Capability

by Berenice Baker
https://www.iotworldtoday.com/quantum/post-quantum-cryptography-gets-performance-testing-capability

Post-quantum cryptography (PQC) helps protect systems from cyberattacks, including those by quantum computers that could break the public-key encryption that currently protects sensitive data.

While sufficiently powerful quantum computers are some years away, organizations are being urged to move toward PQC now to counter hackers stealing data and decrypting it when they are available. These types of cyberattacks are known as harvest (or store) now, decrypt later threats.

The U.S. federal government has mandated the migration of all existing public-key cryptographic systems to PQC. The National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization program has introduced PQC algorithms that will become part of its cryptographic standard.

However, introducing PQC protocols risks slowing network performance and affecting customer experience.

Viavi Solutions, a company that provides network testing and monitoring technology, has added a PQC performance monitoring capability to its TeraVM Security Test software to measure the effect of introducing PQC.

TeraVM Security Test is a software-based test tool that can run on commercial-off-the-shelf (COTS) servers or cloud platforms. It emulates large-scale user endpoint traffic applications over secure access connections and measures individual traffic flow performance.

According to the company, it is the first cloud-enabled test platform to support the PQC algorithms mandated by NIST.

“Our customers have announced significant initiatives to secure their networks from post-quantum threats without compromising their users’ workday experience,” said Ian Langley, Viavi senior vice president and general manager.

“TeraVM Security Test will give them confidence in their capabilities through rigorous testing using standardized algorithms, emulated users, real office applications and loaded networks.”

25.VIAVI Introduces Performance Testing for Post-Quantum Cryptography Deployments

by VIAVI Solutions
https://www.prnewswire.com/news-releases/viavi-introduces-performance-testing-for-post-quantum-cryptography-deployments-302111267.html

Viavi Solutions Inc. (VIAVI) today announced the addition of performance testing capability for Post-Quantum Cryptography (PQC) system deployments. Introducing cryptographic protocols can create additional network performance overhead, ultimately affecting end-user quality of experience. **TeraVM Security Test** is trusted by leading network security infrastructure vendors, service providers, research institutes, governments and enterprises to emulate large-scale user endpoint traffic applications over secure access connections while measuring individual traffic flow performance across multiple quality vectors.

Quantum computers have the potential to break public-key cryptography once they begin operating at a large scale – an event not anticipated to occur for several more years. However, governments, military, enterprises and mobile operators are already preparing for a quantum-safe future to protect their vast stores of sensitive data. The U.S. federal government has mandated the migration of all existing public-key cryptographic systems including network security devices such as firewalls and VPN gateways to PQC.

The race is on for organizations to upgrade their processes, systems, hardware, software and services to avoid Store Now, Decrypt Later (SNDL) threats where encrypted sensitive information can be hacked and stored to be decrypted and acted upon when quantum computers are available.

VIAVI has extensive experience testing and assuring large-scale and complex networks worldwide, including security testing. TeraVM is the first cloud-enabled test platform to support PQC algorithms man-

dated by the U.S. National Institute of Standards and Technology (NIST). TeraVM Security Test enables benchmarking of the performance of enterprise devices, content delivery networks and endpoints that initiate or terminate IPSec Traffic using PQC. TeravVM Security Test is a software-based test tool which can be run on commercial-off-the-shelf (COTS) servers or on cloud platforms. The TeraVM platform is in wide use by network equipment manufacturers, network operators and research institutes for its proven capabilities in testing security compliance as well as performance impacts of security layers.

"Our customers have announced significant initiatives to secure their networks from post-quantum threats without compromising their users' workday experience," said Ian Langley, Senior Vice President and General Manager, Wireless Business Unit, VIAVI. "TeraVM Security Test will give them confidence in their capabilities through rigorous testing using standardized algorithms, emulated users, real office applications and loaded networks."

26.EU Commission Advocates for Post-Quantum Cryptography Adoption

by Igor Nowacki
https://www.dynamikeseidhseis.gr/en/eu-commission-advocates-for-post-quantum-cryptography-adoption/

As quantum computing technology advances, the European Commission has announced a strategic move to protect the European Union's cybersecurity by advocating for a shift to post-quantum cryptography (PQC). This advanced form of encryption is designed to withstand the sophisticated computational powers of quantum computing, which pose a significant threat to current cryptographic standards.

The goal of this initiative is to safeguard sensitive information and to ensure the operational continuity of the EU's digital single market. The Commission's approach focuses on software-based PQC solutions that integrate seamlessly with existing infrastructure, which will facilitate a smooth and cost-effective transition.

The development of PQC is crucial, as it may soon become a vital defense mechanism in an increasingly digitized global economy. The cybersecurity industry is recognizing the potential risks of quantum computing and is making significant strides in creating PQC algorithms capable of resisting quantum decryption methods. While market research forecasts substantial growth in quantum cryptography, the road to mass adoption is lined with challenges including the standardization of algorithms and retrofitting of current systems.

Another concern is the risk of 'harvest now, decrypt later' scenarios, where encrypted data is currently being collected and could be decrypted by future quantum computers. It is therefore imperative to advance to quantum-resistant cryptography as quickly as possible to protect long-standing data confidentiality.

Furthermore, the EU's initiative aligns with international efforts to develop a set of reliable PQC standards. In doing so, the European Commission contributes to a global conversation on cybersecurity and reinforces its commitment to ensuring a secure digital landscape, in partnership with organizations like the National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity.

In summary, the European Commission's dedication to enhancing cybersecurity through PQC adoption

is set to play a transformative role in preserving the digital economy's integrity and security as we approach the quantum computing era.

The European Commission's Initiative on Post-Quantum Cryptography

As the digital era progresses, **quantum computing technology** is evolving at an unprecedented rate, bringing new challenges to the field of cybersecurity. Recognizing the potential threat quantum computers pose to contemporary encryption methods, the European Commission has taken a proactive stance by advocating for a transition to **post-quantum cryptography (PQC)**. This initiative is aimed at protecting sensitive data across the European Union and ensuring the resilience of the digital single market against advanced quantum attacks.

Importance for Cybersecurity and EU Digital Single Market

The adoption of PQC is not merely a preventative measure but a fundamental requirement for future-proofing sensitive information. The auditory goal of the EU's strategy is to fortify cybersecurity defenses to maintain economic stability and privacy. By emphasizing software-based PQC solutions, the Commission is betting on integration that complements existing digital infrastructures, thereby promising a cost-effective and seamless shift.

Market Forecasts and Industry Growth

The global awareness of quantum threats has catalyzed vigorous growth in the **cybersecurity industry**. Market analysts predict a significant expansion in the field of quantum cryptography, fueled by the race to develop secure and efficient PQC algorithms. With heightened interest from both public and private sectors in safeguarding digital assets, the industry is gearing up for a transformative phase.

Challenges and Issues in PQC Adoption

Despite the promising prospects, transitioning to PQC is beset with hurdles such as the need for algorithm standardization and the complexities involved in retrofitting legacy systems. Additionally, the industry must address the concerning strategy of adversaries collecting encrypted data today with the intention of decrypting it with quantum computers in the future, a tactic known as 'harvest now, decrypt later.'

International Collaboration and Standards Development

The EU's initiative on PQC is part of a larger, international effort to define a robust set of PQC standards that can be universally applied. The European Commission is in close collaboration with agencies like the National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity, ensuring that the transition to quantum-resistant algorithms is a collective and globally coordinated endeavor.

Conclusion

The European Commission's commitment to advancing PQC adoption is a strategic response to the imminent quantum computing era. This foresight is instrumental in preserving the integrity and security of the digital economy, safeguarding information against future threats, and reinforcing the EU's role as a leader in digital security on the international stage.

27.Post-Quantum Cryptography (PQC)

by Margaret Rouse
https://www.techopedia.com/definition/post-quantum-cryptography-pqc

What is Post-Quantum Cryptography?

Post-quantum cryptography (PQC) is the development of new cryptographic algorithms that can be used by classical computers and still protect them against the potential threats posed by quantum computing. PQC may also be referred to as **quantum-proof cryptography** or **quantum-resistant cryptography**.

Although quantum computers are still in the early stages of development, they are expected to eventually perform calculations so fast that they can reverse-engineer many of the cryptographic systems currently in use.

The development of secure post-quantum algorithms is a proactive measure to maintain the integrity of sensitive data at rest, data in use, and data in transit and protect it from potential cyberattacks conducted with quantum computers.

Techopedia Explains the Post-Quantum Cryptography Meaning

Cryptography is the science of using mathematical theories and computational algorithms to secure data. Post-quantum cryptography definitions describe a branch of cryptography that focuses on using mathematics to create encryption tools that will work in current IT infrastructures but be resistant to attacks by quantum computers.

Quantum computers are not yet widely available for commercial use due to their high cost and complex operational needs. However, once they reach a sufficient level of maturity and power, quantum computers could break cryptographic algorithms like RSA, ECC, and DSA. This is important because these algorithms are currently used to secure online transactions, email communication, financial data, and other sensitive information.

The Importance of Post-Quantum Cryptography

In 1994, mathematician Peter Shor developed an algorithm that could run on a quantum computer, factor large integers, and compute discrete logarithms exponentially faster than the cryptographic algorithms we are currently running on classical computers.

This was important because the encryption systems we use today rely on the difficulty of factoring large numbers or computing discrete logarithms for their security.

Essentially, Shor's algorithm's success ignited a race against time for cryptography research. Today, researchers focused on data protection are working hard to stay ahead of researchers exploring ways quantum computers can be used to break encryption.

Types of Post-Quantum Cryptography

The National Institute of Standards and Technology (NIST) is playing a leading role in standardizing post-quantum cryptography algorithms.

They are testing and evaluating several types of post-quantum cryptographic algorithms, including:

Lattice-based cryptography	Relies on the difficulty of solving problems in lattice geometry, such as finding the shortest vector in a high-dimensional lattice. Lattice-based algorithms are considered one of the most promising areas for PQC. They are versatile and can be used for encryption, digital signatures, and key exchange protocols.
Code-based cryptography	
Multivariate polynomial cryptography	
Isogeny-based cryptography	
Hash-based cryptography	

How Post-Quantum Cryptography Works

Post-quantum cryptography is not based on the principles of quantum physics. It is based on number theory and the development of mathematical problems that will run on classical computers but be difficult for quantum computers to solve.

The objective is to ensure that encryption remains secure even when quantum as a service (QaaS) becomes widely available. The goal is to create encryption tools that can work within our current digital infrastructure without requiring significant changes.

PQC is still an active research field, and it seems likely there won't be step-by-step directions for how to execute post-quantum cryptography anytime soon.

Implementing Post-Quantum Cryptography

The transition to PQC cryptographic standards is expected to be time-consuming because it involves developing and standardizing new cryptographic algorithms and updating existing systems, infrastructure, and best practices.

When post-quantum cryptography becomes widely adopted, RSA and other classical encryption methods are expected to gradually phase out. In some cases, legacy systems might continue to use traditional encryption standards due to technical or operational constraints. This would likely be in environments considered low-risk, however, or used in situations where updates to post-quantum standards would not be worth it in the short term.

Once PQC algorithms have been standardized, implementation will require collaboration between governments, technology companies, research institutions, and cybersecurity experts. It's expected to be an iterative process that will require careful planning.

PQC algorithms will likely have different performance requirements than current encryption methods. Some algorithms might require more compute resources or memory, and hardware upgrades or algorithm optimizations might be needed to avoid performance bottlenecks and ensure smooth operation.

Security Considerations in Post-Quantum Cryptography

Data in sectors like healthcare, finance, and government is often archived and may need to remain in secure storage for decades because of compliance regulations.

There's a real risk that adversaries will collect encrypted data now with the intent to decrypt it later using

quantum computers. This strategy, which is known as “harvest now, decrypt later,” is an important consideration for PQC researchers.

In the future, certain industries are likely to be mandated to use post-quantum cryptography to achieve the desired security level for confidentiality, integrity, and authenticity (CIA).

The Challenges of Post-Quantum Cryptography

The biggest challenge moving forward will be to figure out which new cryptographic algorithms are most resistant to quantum attacks and can be integrated into existing systems with minimal disruption.

You can expect the process of standardizing post-quantum cryptographic algorithms to be lengthy and complex. It will involve policy changes, regulatory changes, and logistical coordination across countless organizations, governments, and industries worldwide.

Technical issues related to performance are another concern. Some post-quantum algorithms will require larger encryption key sizes, which has implications for bandwidth and storage requirements.

Considerations will also need to be made for Industrial Internet of Things (IIoT) environments whose embedded systems and IoT devices have limited processing and storage resources. In this use case, the impact on system performance and interoperability between systems using different PQC standards will have to be carefully evaluated to ensure practicality. This will involve extensive testing, evaluation, and consensus-building among cryptographic researchers, industry stakeholders, and standardization bodies.

Pros and Cons of Post-Quantum Cryptography

Like any technological shift or digital disruption, PQC comes with its set of advantages and challenges. Here are some of the pros and cons:

Pros

- ✓ Resists classical and quantum attacks
- ✓ Secures future and archived data
- ✓ Boosts new cryptography research
- ✓ Ensures vetted, secure, practical algorithms through standardization

Cons

- ✗ Requires larger keys and more computational resources
- ✗ Presents a steep learning curve due to new PQC math problems
- ✗ Challenges integration with old systems
- ✗ Lacks the extensive testing of classical algorithms
- ✗ Necessitates software upgrades and personnel training for transition
- ✗ Exhibits limited expertise among developers, cybersecurity professionals, policymakers

Future of Post-Quantum Computing

Post-quantum cryptography is a relatively new field. While many promising algorithms already exist, they have not undergone the same level of rigorous scrutiny as established classical cryptography methods. Careful and ongoing evaluation will be needed to identify any potential vulnerabilities or weaknesses before these algorithms are widely deployed in critical systems.

While NIST is evaluating the effectiveness of PQC algorithms and deciding which one to standardize, organizations can use the time to conduct a security audit and create a reference index for programming and application software that uses encryption. Once the strategies for post-quantum cryptography implementation have matured and a standard has been approved, the index can be used to develop a plan for how to upgrade or replace applications that require cryptography.

Quantum Computing vs. Post-Quantum Computing

When discussing PQC, it's important to understand that "post-quantum cryptography" and "quantum cryptography" are not synonyms, even though the two terms sound similar.

Quantum cryptography (QC) researchers are investigating ways quantum physics can be used to secure communication. They are researching quantum key distribution (QKD) and ways the behavior of photons (light particles) can prevent eavesdroppers from intercepting communications without being detected. QKD is currently one of the most well-developed, practical applications of quantum cryptography today.

In contrast, the post-quantum computing meaning is focused on mathematics and developing new algorithms. It is an effort to protect sensitive data in a future where quantum computers are an everyday reality.

The Bottom Line

PQC researchers are developing new cryptographic algorithms that classical computers can use, but quantum computers can't break. This initiative is in response to the discovery of Shor's algorithm, which could theoretically break the cryptographic schemes currently in use.

28.Live QKD demonstrations at OFC Conference

by IDQ
https://www.idquantique.com/live-qkd-demonstrations-at-ofc-conference-2/?utm_term=Live%20QKD%20demonstrations%20delivered%20at%20OFC%20Conference%20and%20Exhibition&utm_campaign=Quantum%20Era%20Security%20Times%3A%20April%202024&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%3A%20April%202024-_-Live%20QKD%20demonstrations%20delivered%20at%20OFC%20Conference%20and%20Exhibition

The Optical Fiber Communication Conference and Exhibition (OFC) 2024 is one of the largest technical conference and exhibition experiences in the telecom world. The 2024 edition took place in SanDiego last week and it was a special one for ID Quantique.

The most important aspect was to demonstrate the integration of QKD with equipment manufacturers. The specificity of OFC, starting from last year, is that it offers a dedicated optical fiber network, **OFCNet,** which is used for demonstrations highlighting new technologies. We took advantage of this to build two QKD-secured links between our booth and the booths of both Ciena and Nokia. There was a lot of interest from visitors. The fact that a QKD network can be installed easily in this com-

plex environment is a demonstration of how far we have gone towards integration of QKD in the telecom world.

On the technical side, we contributed to 6 panels and presentations over the whole conference. The most relevant progress we saw, was the **demonstration of outstanding hollow core fiber performance**. These fibers, where light actually propagates mostly in air, with some glass surrounding it to guide it, may revolutionize the telecoms. They already achieve lower loss than the best glass fiber, with no non-linear interactions between different wavelengths. This will mean for quantum communications a single fiber, propagating both the quantum and all the classical signals without a compromise on longer distances; which will be a significant improvement for long distance QKD.

A couple of recordings are already available on the OFC webiste. We are happy to point out to 2 where IDQ contributed:

Workshop: How Can OFC, with a Real Life Test-Bed, Accelerate Innovation in the Optical Photonic Networks?

Workshop: QKD – An End-Game or Just a Stepping Stone to the Quantum Internet?

