Crypto News

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

May 01, 2022

1.Editorial

Our goal as the CSA Quantum Safe Security working group is to share information with you about current and future implications of quantum computing in all aspects, but specifically to those related to the discipline of security. It's to discuss questions such as, what are our adversaries doing now with our encrypted information to prepare it for a post- quantum world? What can we do now to prepare for these current and on-going attacks as well as those looming in the not too distant future? Should I be worried or is there hope? If you're interested in an overview, hop over to articles 7 and 9 to get answers to these and other pressing questions you may have.

Now that you have some background, you likely accurately surmised that the entire world is interested in quantum computers for a variety of reasons and uses. One focus is for military advancement. Article 29 has information about how different nations are working together on this effort. Want a broader perspective of the "types" of problems quantum computers can solve? How about 10 of them? Article 39 outlines the top 10 problems that previously seemed difficult but with quantum computers will be relatively easy.

What other articles did you find interesting? I'd love to discuss it with you so feel free to reach out. Happy reading!

Crypto News is authored by Dhananjoy Dey with this editorial provided by Mehak Kalsi. Both are active members of the Cloud Security Alliance (CSA) Quantum-Safe Security Working Group (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.

2.A New Vulnerability Threatens Three Finalists of The Nist Post-Quantum Cryptography Contest

by IDQ

https://www.idquantique.com/new-vulnerability-threatens-three-finalists-nist-pqc-contest/?utm_term=Read%20more&utm_campaign=Quantum%20Era%20Security%20Times%20April%202022&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%20April%202022-_-Read%20more

At the beginning of April 2022, the Center of Encryption and Information Security (an information security unit within the Israeli Defence Force) published a report on the security of Learning with

Errors (LWE) and Learning with Rounding (LWR) based algorithms. The report is of particular interest because three of the six shortlisted finalists in NIST's post-quantum cryptography standardization project are LWE/LWR based.

The report shows that the application of some improvements to a specific attack type (known as a dual lattice attack) significantly reduces the security of the shortlisted algorithms – to the point that they fall below NIST's required security threshold. The claim is, of course, under scrutiny by the community.

Abstract

> "Many of the leading post-quantum key exchange and signature schemes rely on the conjectured hardness of the Learning with Errors (LWE) and Learning with Rounding (LWR) problems and their algebraic variants, including 3 of the 6 finalists in NIST's PQC process. The best-known cryptanalysis techniques against these problems are primal and dual lattice attacks, where dual attacks are generally considered less practical.
>
> In this report, we present several algorithmic improvements to the dual lattice attack, which allow it to exceed the efficiency of primal attacks. In the improved attack, we enumerate over more coordinates of the secret and use an improved distinguisher based on FFT. In addition, we incorporate improvements to the estimates of the cost of performing a lattice sieve in the RAM model, reducing the gate-count of random product code decoding and performing less inner product calculations.
>
> Combining these improvements considerably reduces the security levels of Kyber, Saber and Dilithium, the LWE/LWR based finalists, bringing them below the thresholds defined by NIST."

3.Quantum Computing Review Q1 2022

by IDQ

https://www.idquantique.com/quantum-computing-review-q1-2022/?utm_term=Quantum%20Computing%20Review%20Q1%202022&utm_campaign=Quantum%20Era%20Security%20Times%20April%202022&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%20April%202022-_-Quantum%20Computing%20Review%20Q1%202022

Welcome to our Q1 2022 quantum review. As we move further into the quantum decade, investment and advancement in quantum technologies continues apace. What follows is just a small selection of the quantum stories making the news in recent months.

The countdown to quantum

In March the Cloud Security Alliance (CSA) started its "countdown to quantum". April 14, 2030 has been set as the date by which the CSA estimates a quantum computer will be able to break today's

cybersecurity infrastructure. The CSA website now features a Y2Q countdown clock as a sober reminder of the imminent threat posed by quantum computing. Somewhat dramatically, the CSA has nicknamed it the countdown to quantum destruction.

A matter of principle

Earlier in the year, the World Economic Forum published an insight report into Quantum Computing Governance Principles. The report recognises "there is a need for global guidelines to assess and manage the opportunities and risks of quantum computing".

In the report, the authors identify 9 core themes that define the overarching principles:

- Transformative capabilities
- Access to hardware infrastructure
- Open invitation
- Creating awareness
- Workforce development
- Cybersecurity
- Privacy
- Standardization
- Sustainability

A qubit by any other name

According to a recent research blog by Microsoft, researchers into quantum computing are frequently frustrated by the lack of scalability inherent in current computing models. Today's quantum computers are built on a variety of qubit types, but none of them are scalable to the point that quantum computers make a substantial leap forward.

So, Microsoft have taken the decision to pursue a different approach and utilise topological qubits. Topological qubits are (at least in theory) more stable than other qubits and should make scale more viable.

Movers, shakers and money-makers

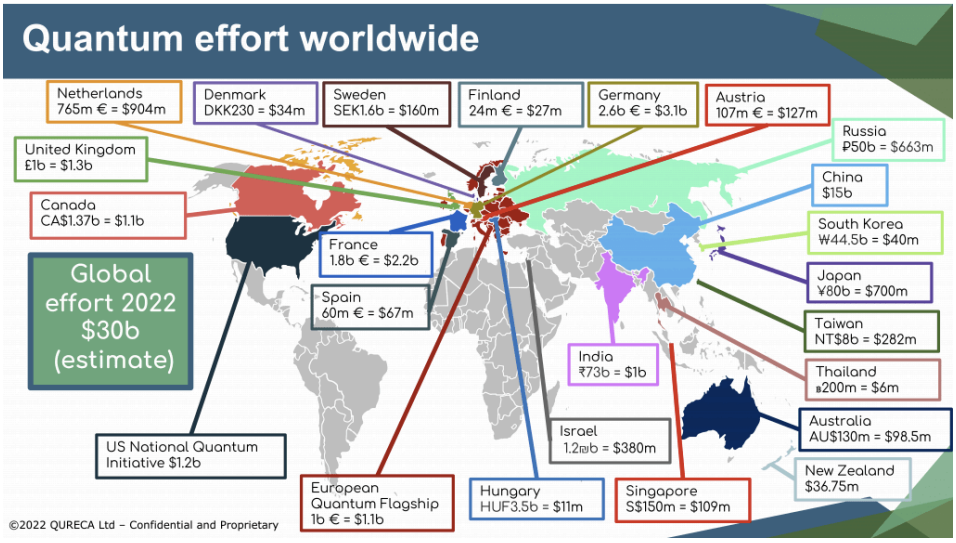
As the quantum technology marketplace expands, it undergoes a period of dynamic investment and merger activity. One of the prominent names in the fledgeling industry has been Rigetti Computing, and they made the headlines again in March. In what is described as a Business Combination with Supernova Partners Acquisition Company II Ltd, Rigetti received circa $260million. The company plans to use the proceeds to accelerate its development of future generations of quantum processors and to expand its operations.

Not to be outdone by the private sector, a number of governments announced significant investments in quantum technologies in Q1. France announced it was to invest over €70million in a new National Quantum Computing Platform.

At the same time, Germany is looking to advance its quantum computing roadmap with the introduction of QuaST – the Quantum-Enabling Services and Tools for Industrial Applications. The consortium is designed to facilitate rapid adoption of quantum technologies and has already attracted €5.5million in funding.

Still in Germany, the Federal Ministry of Education and research has announced €16milion in funding for a project called PhotonQ. The project will see a group of seven academic and commercial institutions working to develop a range of photonic technologies, including deterministic photon sources, scalable silicon photonic circuits and novel single-photon detectors. Finally, 25 German research institutions and companies are working on the QSolid project to build a quantum computer with improved error rates. The five-year project has a budget of over €76million.

This handy graphic, courtesy of QURECA, summarises the main programs in place across the world.



Other News

In January, Capgemini announced it was launching a dedicated quantum lab and signed an agreement with IBM to advance industry applications of quantum computing.

In February, IonQ announced its latest quantum computer (IonQ Aria) had achieved a record 20 algorithmic qubits; reinforcing its claim to be the most powerful quantum computer in the industry.

In March, HSBC also announced a partnership with IBM to explore further applications of quantum computing in the financial services marketplace.

4.SK Telecom and Samsung Unveil The Galaxy Quantum 3, The World's Most Secure

5G Smartphone Featuring IDQ'S QRNG Chip

by IDQ

https://www.idquantique.com/sk-telecom-and-samsung-unveil-the-galaxy-quantum-3-world-most-secure-5g-smartphone-featuring-idq-qrng-chip/?utm_term=SK%20Telecom%20and%20Samsung%20unveil%20the%20Galaxy%20Quantum%203%2C%20the%20world%5Cu2019s%20most%20secure%205G%20smartphone%20featuring%20IDQ%5Cu2019s%20QRNG%20chip&utm_campaign=Quantum%20Era%20Security%20Times%20April%202022&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%20April%202022-_-SK%20Telecom%20and%20Samsung%20unveil%20the%20Galaxy%20Quantum%203%2C%20the%20world%5Cu2019s%20most%20secure%205G%20smartphone%20featuring%20IDQ%5Cu2019s%20QRNG%20chip

The new Galaxy Quantum 3 is equipped with the world's smallest (width 2.5 x length 2.5mm) Quantum Random Number Generator (QRNG) chipset designed by ID Quantique, enabling trusted authentication and encryption of information allowing smartphone holders to use applications and services in a safer and more secure manner by generating unpredictable and patternless true random numbers.

In this new phone, IDQ's QRNG chip enhances the security of a large number of services provided by the operator. Quantum random Number Generators protect the process from log-in/authentication/payment/unlock/OTP generation of service apps ranging from financial apps to social media apps and games offering a much higher level of trust to the users. The QRNG is also used to encrypt data stored in the external memory card.

In addition, for the first time in the series, 'Galaxy Quantum 3' offers a differentiated security experience to customers by providing a 'quantum indicator' on the status bar so that customers can realize that they are using a quantum security service.

We expect that the Galaxy Quantum 3 will become the safest and most reliable device in these days where financial transactions through smartphones are essential. We will continue to achieve innovations to provide customers with more safe and secure services.

Bong-ho Lim, Chief Mobile Officer (CMO) of SKT

The Galaxy Quantum 3's native integration of the QRNG chip automatically enhances the security of a larger number of services used on the smartphone bringing applications and services to a new level of security in the mobile phone industry.

Grégoire Ribordy, CEO and co-founder of ID Quantique

5.In praise of the Feistel network

by Simson Garfinkel
https://www-technologyreview-com.cdn.ampproject.org/c/s/www.technologyreview.com/2022/04/27/1048456/in-praise-of-the-feistel-network/amp/

On March 17, 1975, the National Bureau of Standards (NBS) published its proposed Data Encryption Standard (DES) in the Federal Register. The algorithm used a 56-bit encryption key, which (it was hoped) meant there was no possible way for an attacker to decrypt the resulting ciphertext without setting out to try each of the 72,057,594,037,927,936 possible keys one by one.

DES was based on a revolutionary new approach to encryption developed at IBM by Horst Feistel '37 and published in the May 1973 Scientific American. But while the 1973 article provided merely a broad outline of his approach, the DES publication contained step-by-step instructions for building a strong encryption system that businesses and individuals could use.

The advent of shared computing in the early 1970s made it clear that government agencies, banks, and other organizations needed to protect their data, but most of the good information about encryption was locked up inside the National Security Agency. Though a variety of proprietary systems were on the market, few people outside the NSA knew what made a strong encryption algorithm and what was junk.

What the government needed was a single, strong standard that would create trust and help the growing information technology market thrive. So NBS solicited encryption algorithms from the public, and IBM ultimately submitted two of Feistel's: first one with a 128-bit key he called Lucifer, and then, after some back-and-forth, what became DES.

Given that context, the NBS's choice was perplexing. On the one hand, DES did deliver on its promise: after decades of analysis, there is still essentially no way to decrypt DES-encrypted data other than potentially trying every key, in what's called an "exhaustive search." But on the other hand, one would expect that the 56-bit key would be nowhere near as strong as the 128-bit Lucifer.

Mounting an exhaustive search against DES was at the edge of possibility in 1975. Martin Hellman, a professor of computer science at Stanford University, and Whitfield Diffie '65, a researcher in Hellman's lab, estimated that for $20 million the US government could build a machine capable of trying all possible keys; adding just eight more key bits would increase the difficulty by a factor of 256, making a key search practically impossible. It was as if the proposed standard had been carefully designed so that DES-encrypted messages could be cracked by the US government but not by US corporations.

Fleeing Hitler

Feistel was born in Germany in 1915 into a middle-class Protestant family. His aunt married a wealthy German Jew named Franz Meyer, and the two fled Germany for Zürich, Switzerland, before 1931.

When Hitler came to power in 1933, Feistel was terrified that compulsory military service would be reinstated (which it was). So his uncle devised a plan to have Feistel attend summer school at Columbia

University in 1934 to improve his English, then enroll at the Eidgenössische Technische Hochschule (ETH) in Zürich for college, and finally transfer to a university in the US to complete his studies and obtain permanent residence. The plan worked, and Feistel entered MIT in the fall of 1936. Meyer and his wife followed, moving to New York City before 1940.

Feistel graduated from MIT in 1937 with a degree in physics and continued as a graduate student until 1938, when he enrolled at Harvard. He became a US citizen on January 31, 1944. "The following day, he told me, he was given a top secret clearance," recalls Diffie. Yet Feistel felt that he experienced discrimination because of his German heritage. Although he had been interested in codes and cryptography since he was a child, he couldn't work on them. "He said something to someone during the war and was told that 'it was not the time for a German to be talking about cryptography,'" Diffie recalls.

A career in cryptography

Finally, he got his chance. After working at the MIT Radiation Laboratory, Feistel got a job at the Air Force Cambridge Research Center (AFCRC), which had been asked to evaluate an Identification Friend or Foe (IFF) system that aircraft used to identify themselves to radar systems so as not to be shot down.

Feistel's group found a flaw with the system and developed a better approach based on cryptography. It's not clear whether it was ever deployed: within a few years, the AFCRC cryptography group was shut down, likely because the Department of Defense was centralizing cryptographic research at the NSA. But modern IFF systems do employ cryptography and a key that is changed regularly.

In November 1957 Feistel took a job at MIT Lincoln Laboratory, where he wrote a report summarizing the IFF work done at AFCRC. "Whatever the particular application may be, any scheme of secret communication should be carefully analyzed and evaluated for its merits and faults," he concluded. "It is better to know where one stands, than being SPOOFED into a false sense of security, through lack of knowledge or perhaps even inventor's pride."

Lincoln didn't work out for Feistel, though, and neither did MITRE, the Bedford-based research firm, where he went in 1961. "My father wasn't very happy there," recalls his daughter, Peggy Chester: again, Feistel thought colleagues discriminated against him because he was German. Feistel took pride in his German heritage and in German engineering, says Harold Mattson, PhD '55, who worked with Feistel at AFCRC. He adds that Feistel was also somewhat bitter about the postwar world order, describing the United Nations as a "Victors' Club" on more than one occasion.

It may have been during his years at MITRE that Feistel developed his encryption approach. But if so, he didn't share it. "He was very cautious about revealing his Lucifer code," his daughter says. "He was afraid that other people would take it from him." It's also possible that cryptography work he wanted to do at MITRE was being stifled by the NSA.

In 1968, Feistel moved to IBM, which hired him specifically to work on cryptography for commercial applications. It's here that he likely perfected his encryption algorithm. On June 30, 1971, the company filed a patent application for his "Block Cipher Cryptographic System." NSA reviewed the application

and issued a secrecy order blocking publication of the patent—but NSA's order, dated October 17, 1973, was five months after the Scientific American article. NSA's order was rescinded on November 14, 1973, and US Patent 3,798,359 was published on March 19, 1974, with H. Feistel listed as the inventor.

"Horst was key to the IBM cryptographic research effort," says Hellman, who also taught at MIT from 1969 to 1972. "In 1973, when Horst published that paper, it was an eye-opener for many of us. It opened an approach to cryptography that made a lot of sense." Today the approach is so identified with Feistel that the basic design of DES and other similar algorithms is called a "Feistel network."

Meanwhile, Diffie and Hellman discovered public-key cryptography in 1976. One of its primary uses is to distribute encryption keys for algorithms like DES.

Putting DES to rest

Work by Don Coppersmith '72 published in the IBM Journal of Research and Development in 1994, four years after Feistel's death, revealed that IBM knew by 1975 that the 128-bit Lucifer key would have been vulnerable to differential cryptanalysis, a cryptanalytic attack independently discovered by academics in the late 1980s. In the process of strengthening Lucifer, IBM shortened the key. In other words, when DES was approved for use in the 1970s, it might have been stronger than Lucifer after all.

But by the mid-1990s, computer scientists widely acknowledged that the 56-bit key was no longer secure and argued that DES should no longer be used to protect information.

To demonstrate that US policy was putting privacy at risk, in 1998 the Electronic Frontier Foundation constructed a machine called Deep Crack that cracked a DES-encrypted message in just 56 hours. The machine cost $250,000 to build, but most of that was engineering costs: EFF estimated that the second machine would cost less than $50,000.

"Our research results prove that DES can be cracked quickly on a low budget," the EFF book Cracking DES concludes.

DES was replaced by a new algorithm called the Advanced Encryption Standard (AES) on May 26, 2002. As near as anyone knows, AES is still secure.

6.BT and Toshiba Launch First Commercial Trial of Quantum Secured Communication Services

by Matt Swayne

https://thequantuminsider.com/2022/04/27/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services/?utm_source=newsletter&utm_medium=email&utm_term=2022-04-30&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Quantum+Comm+Commercialized+Non-Nerds+Need+Apply+--+And+More+Quantum+News

At an event held at BT Tower, BT and Toshiba, along with EY launched the trial of a world first commercial quantum secured metro network. The infrastructure will be able to connect numerous customers across London, helping them to secure the transmission of valuable data and information between multiple physical locations over standard fibre optic links using quantum key distribution (QKD). QKD is an important technology, playing a fundamental role in protecting networks and data against the emerging threat of cyber-attack using quantum computing. The London network represents a critical step towards reaching the UK government's strategy to become a quantum-enabled economy.

The network's first commercial customer, EY, will use the network to connect two of its sites in London, one in Canary Wharf, and one near London Bridge. It will demonstrate how data secured using QKD can move between sites and will showcase the benefits this network brings to its own customers.

BT and Toshiba announced their commitment to creating a trial network in October 2021. BT will operate the network, providing a range of quantum-secured services including dedicated high bandwidth end-to-end encrypted links, delivered over Openreach's private fibre networks, while Toshiba will provide quantum key distribution hardware and key management software. In the network, QKD keys will be combined with the in-built ethernet security, based on public-key based encryption, which will enable the resultant keys to be used to encrypt the data.

George Freeman, Minister for Science, Research and Innovation, HM Government, commented: "I am very pleased to see the first trial by BT and Toshiba of a commercial quantum secured metro network, which represents significant progress towards achieving our ambition to make the UK a quantum-enabled economy. This is the kind of innovation that helps cement the UK as a global innovation economy in the vanguard of discovering, developing and commercially adopting transformational technology with real societal benefits."

Howard Watson, Chief Technology Officer, BT, commented: "Quantum-enabled technologies are expected to have a profound impact on how society and business operates in the future, but they are remarkably complex to understand, develop and build: in particular, ensuring that the end-to-end service designs meet the stringent security requirements of the market. I'm incredibly proud that BT and Toshiba have successfully united to deliver this unique network, and with EY as our first trial customer, we are paving the way for further commercial explorations for quantum technologies and their use in commercial, and societal applications in the future."

Shunsuke Okada, Corporate Senior Vice President and Chief Digital Officer of Toshiba commented: "Both Toshiba and BT have demonstrated world-class technology development and leadership through decades of innovation and operation. Combining BT's leadership in networks technologies and Toshiba's leadership in quantum technologies has brought this network to life, allowing businesses across London to benefit from quantum secured communications for the first time."

Preparation, technical deployment and testing for the network commenced in late 2021. This included equipment deployment in racks, adding security systems and resilience testing, and finally running and optimising the network. While Tuesday 26th April marked the official launch of the network, it has been running since early April, and will operate for an initial period of up to three years.

Praveen Shankar, EY UK & Ireland Managing Partner for Technology, Media and Telecoms (TMT), commented: "Quantum technology creates new and significant opportunities for business, but presents potential risks. Quantum secure data transmission represents the next major leap forward in protecting data, an essential component of doing business in a digital economy. Our work with two of the world's leading technology innovators will allow us to demonstrate the power of quantum to both EY and our clients."

The UK Government's "strategic intent" to develop a quantum-enabled economy was first published in 2020. It sets out a vision for the next 10 years in which quantum technologies will become an integral part of the UK's digital backbone, unlock innovation to drive growth and help build a thriving and resilient economy, and contribute significant value to the UK's prosperity and security.

The London network represents an important step to building a national network for quantum secured communications, which will stimulate the growth of a quantum ready economy in the UK.

Howard Watson continued: "This is a significant moment in the UK's journey towards a quantum-enabled economy, but we're not there yet. Further investment commitments will be required to broaden the study of quantum technologies that will contribute to this new economy, including quantum computing, quantum cryptography and quantum communications. We look forward to working with our government and industry partners to continue the momentum BT has started and shaping the UK's quantum strategy."

The technical collaboration for this network was conducted in BT's Adastral Park labs in Suffolk, UK, and the Quantum technology Business Division of Toshiba, based in Tokyo, Japan and Cambridge, UK, where the quantum key distribution technology has been developed and is manufactured.

7.The Quantum Cryptography Conundrum

by Kimberly Underwood
https://www.afcea.org/content/quantum-cryptography-conundrum

Time is of essence in preparing for quantum-resistant cryptography, leader says.

The United States is developing new algorithms to protect against the adversary's future—powerful quantum computing that will be able to break into currently encrypted systems and data. Led by the NIST, seven advanced algorithms are being considered for use as standardized methods. The Defense Information Systems Agency, or DISA, is working with NIST and Defense Department leaders to implement the quantum-resistant cryptography solutions, when ready, into military use, said Deepak Seth, DISA's chief engineer, Emerging Technologies Directorate.

The chief engineer spoke on April 27 at AFCEA's TechNet Cyber conference in Baltimore, being held April 26-28.

"Quantum computers offer great promise," Seth acknowledged. "We hear about them all the time. They promise to really revolutionize computing. They offer breakthroughs in science and engineering. But while it's an exciting new technology, it also poses a serious security threat. When these computers become operational, our current asymmetric encryption technology today will be rendered insecure."

Presently, for authentication means, digitally signing documents, sending encrypted messages or encrypting data, the DoD uses asymmetric encryption, Seth explained. "Asymmetric encryption is really the foundation element of our public key cryptography," he said.

The problem is that these current security mechanisms will not be effective in protecting data from quantum-based attacks, whenever they are operational, whether that is in five, 10 or 15 years. And adversaries could already be taking hold of encrypted information to be broken into later.

"We presume that our adversaries are executing these so-called 'store now and decrypt later' attacks, in which they are basically harvesting our encrypted data that flows across the networks and across the Internet," Seth emphasized. "Adversaries are harvesting it. They are storing it and hoping that when they get their hands on a quantum computer in the future that they'll be able to decrypt the data and then be able to see what current messages were."

Even the well-known Shor's algorithms will be able to be broken by quantum computers. "If a Shor's algorithm were to run today on a quantum computer, the time it would take to decrypt the data would be shortened from years to days and even possibly less," Seth warned. "It is for this reason and many others that DISA is extremely concerned about the threat posed by quantum computing."

NIST has already identified seven possible quantum resistant algorithms that could be used to protect against quantum computer-based attacks. Of those seven solutions that appear to have the most promise, the agency will select a final algorithm to be considered for standardization—following the end of NIST's third round of competition.

"Once these new algorithms are announced and when they are standardized, DISA intends to adopt these NIST standardized, quantum-resistant algorithms for our public key infrastructure," Seth explained.

Time is of the essence, the chief engineer stressed. DISA and officials across the DoD must start to examine now how they will integrate the quantum-resistant algorithms into their existing networks and operations.

"We have to prepare ourselves now for integration to be able to use these new encryption algorithms," Seth said. "It has taken us years to field new security solutions into DoD networks and IT systems and to make things worse, these new NIST quantum-resistant algorithms will not be as simple as 'swap out, swap in' or a drop-in replacement."

Moreover, the new algorithms won't be a static solution. "It's also expected that some of these algorithms will change overtime," Seth realized. "There will be new variants to these algorithms and some modifications, so we also will need the ability to quickly upgrade new cryptography into our IT infrastructure."

In addition, the chief engineer advised that organizations start considering post-quantum algorithms and the associated need for updates to infrastructure as part of a modern development security operations, or DevSecOps, software development process.

"It's a really serious problem," he stressed. "We have to prepare now to begin to adopt quantum-resistant algorithms and we must do so at the earliest possible time to protect our data from quantum attacks."

8.Security Teams Should Be Addressing Quantum Cyber-Threats Now

by James Coker

https://www.infosecurity-magazine.com/news/security-teams-quantum-cyber/

Addressing quantum cyber-threats should already be a high priority for cybersecurity professionals, according to Duncan Jones, head of cybersecurity at Quantinuum, speaking during the ISC(²) Secure Webinar 'The Threat and Promise of Quantum Cybersecurity.'

Jones began by emphasizing the significant differences between quantum and classical computing, both in operations and possibilities. One of the most significant of these is that while classical computers only have binary choices, 0 or 1, quantum computers are made up of 'qubits,' which "can have values that are combinations of 0 and 1." This mixture is known as a 'superposition.'

This enables calculations to be made in parallel. In addition, qubits can be connected, which provides the opportunity to model aspects of nature in their entirety. This aspect offers enormous potential in fields like drug discovery, where testing could be simulated rather than requiring lengthy and expensive trials.

Jones added that many companies operating in this space are developing different types of computers. "It's unlikely that one technology will emerge as the best answer in every situation. I think in the years ahead, we'll have different types of quantum computers for different purposes," he stated.

However, quantum also poses significant dangers in cyberspace. In particular, in the next 10-15 years, it is expected to be able to break existing cryptography algorithms such as RSA, Elliptic curve cryptography and Diffie-Hellman key exchange. For example, quantum algorithms like Shor's algorithm (1994) will ultimately solve the complexities of such systems.

This threat is not imminent, and Jones said we are currently in the noisy intermediate-scale quantum (NISQ) era, in which the leading quantum processors do not contain enough qubits to mount such attacks. However, this will inevitably change in time, and the asymmetric realm "will be completely broken by Shor's algorithm."

This will impact numerous everyday systems, including public key infrastructure (PKI), HTTP/TLS, network security, payments, Internet of Things (IoT) and blockchain.

Jones emphasized that quantum does not just represent a future cyber-threat but nevertheless is very relevant today. This is the concept of 'hack now, decrypt later.' In this scenario, a hacker will listen in to and record an encrypted exchange today, which they can decrypt retrospectively on a quantum computer in the future. Therefore, "perfect forward secrecy doesn't help you here because the attacker can see all the messages that were exchanged, and a quantum computer will be able to break the mathematics protecting that exchange." This issue is particularly pertinent to data that will still be relevant in 10-15 years, such as health information. "Quantum attacks may well have already started," noted Jones.

He also highlighted the huge dangers quantum attacks pose to IoT devices. This is because these devices have a secure boot mechanism baked into the silicon that cannot be upgraded, leaving many of these devices vulnerable to quantum attacks. "What happens if you've got a device in 30 years' time that has an elliptic curve-based secure boot mechanism in the field?" he asked.

Despite these concerns, Jones emphasized that there are actions security teams can take now to secure their systems against the threat of quantum. He highlighted the National Institute of Standards and Technology (NIST)'s ongoing process to identify new algorithms "that we don't think a quantum computer can solve any better than a classical computer." It is currently at round three, a stage that will decide the algorithms selected for standardization.

Jones added that we have been "spoilt" by algorithms like RSA, which provides both digital signatures and encryption. However, post-quantum algorithms will not be able to do both, with different algorithms required for different problems. Therefore, NIST is seeking separate algorithms for public key enabling (PKE) and digital signatures. Once round three has closed, the 'winners' will proceed to standardization, with the final standards set to be finalized in 2024. In addition, round four will subsequently try and identify further potential candidates.

Jones said that organizations should consider moving to a 'hybrid mode' regarding their cryptographic algorithms, in which a post-quantum algorithm is combined with classical algorithms. This "makes you no less secure than just using your classical algorithm, but if you chose a good candidate that turns out to be quantum-resistant, it protects you against this hack-now-decrypt-later concept." He noted that some systems and products are already moving in this direction. Currently, this should be done in a closed eco-system in the absence of standardization.

Jones went on to discuss how security teams can migrate to post-quantum cryptography, noting "there are a lot of steps ahead of us." He cited NIST, which believes full implementation of a new crypto standard will take a decade or more. For now, teams should be focusing on understanding the cryptography they are using, the highest-value assets in their organization and the assets most vulnerable

to being recorded today and decrypted later.

He added that organizations should be communicating to their cybersecurity vendors about this issue, "asking them what their quantum-safe roadmap looks like."

The potential cybersecurity benefits of quantum computing were also highlighted by Jones. These revolve around two main areas: quantum key distribution and quantum key generation. "In some areas of cybersecurity, we can actually throw away those complexity assumptions and instead build systems that have no complexity assumptions at all," he said.

A number of organizations are working on developing systems based on this principle, including Quantinuum.

Concluding his presentation, Jones offered the following advice to security teams regarding addressing quantum threats:

- Understand your assets and use of cryptography
- Identify the biggest risks (sensitive data, hack now, decrypt later)
- Speak to vendors – ask them about their quantum-safe roadmap
- Create a prioritized migration plan
- Test and experiment as soon as possible

9.Something Has to Be Done About The Quantum Computer Security Threat

by Chris Szewczyk
https://www.pcgamer.com/something-has-to-be-done-about-the-quantum-computer-security-threat/

When it comes to technology, revolutionary is a word that gets overused. But if there's one thing in the world of 21st century computing that will deserve being described as such, it's a fully functional quantum computer. It's no exaggeration to suggest that quantum computers have the potential to change the world as we know it.

Quantum computers are coming sooner than you might expect, in fact there are already functional, if rudimentary systems that have been developed by giants including IBM, Microsoft and Google along with many others. And you can be sure that the governments of the world are working behind the scenes in a quantum arms race. What we see in public is likely not at the bleeding edge of quantum computing research and development.

The power of a quantum computer, versus that of a classical computer—or QC vs PC—is they're set to dramatically advance fields as diverse as climate science, biology, and machine learning. But there's another application, and it's a somewhat shady one: espionage.

The governments of the world see quantum computers as a tool to break encryption standards. A fully functioning and stable high qubit quantum machine has the potential to wreak havoc across the internet. Previously secure networks would be vulnerable and public confidence in financial systems could collapse.

Forget Y2K, think Y2Q.

Then there are cryptocurrencies. Quantum computers could pose an existential threat to crypto, but I'll get to that a bit later. First, a crash course in quantum computing.

What is a quantum computer?

The functions of a classical computer are based around the use of bits, or binary digits, represented by 1s or 0s. A quantum bit, or a qubit as it's known, can exist as a 1 or 0, or both at the same time. This makes a QC much more adept at seeking answers to problems with a large number of outcomes or possible combinations than a classical computer.

A qubit harnesses the properties of quantum superposition. Via quantum entanglement, a qubit can be linked to other qubits to exponentially increase processing power. In simple terms, a QC is excellent at leveraging probabilities, which means that the answers to complex operations are exponentially faster with more qubits. A QC with enough qubits is capable of certain computations that a classical computer can never realistically solve. In certain cases, a calculation that a quantum computer could complete in mere minutes may take billions of years, or more to solve on even the world's most powerful supercomputer today.

The point at which a quantum computer can outperform a classical computer is called quantum supremacy. Some researchers already claim it has occurred, but any such claim is very specific, and completely impractical in a real world sense. There are also significant challenges to overcome before quantum computing becomes a commercial reality. Qubits are tricky things, to put it mildly, and maintaining coherence and scaling them is an area of ongoing research.

It's likely that we're many years away from practical quantum computers, but with enough stable qubits, there are some genuinely world-changing possibilities within reach. For now, the one I'll focus on is the ability to crack encryption. That might be the number one reason for governments to develop quantum computers.

The security of the internet is vulnerable

It goes without saying that there's a need for network security. Military networks, financial systems, critical infrastructure, communications. You name it, it all needs to be secure to maintain confidence in the system. Security is built upon encryption.

Much of the encryption underpinning internet security is based upon prime numbers. As far back as 1994, American mathematician Peter Shor developed what is known as Shor's algorithm. It is used to find the prime factors of an integer. Put simply, this algorithm can be used to break many public key

cryptography schemes, including RSA, one of the most widely used, and oldest algorithms for encryption.

I don't mean to be a scaremonger here. A QC capable of breaking a large key RSA encryption is probably years away at best, but the theoretical vulnerability exists, and the time to protect the possibility of an attack against it is now.

The governments of the world are developing post-quantum encryption schemes. US NIST is undertaking a multi-year project with the aim of standardizing one or more quantum-resistant public-key cryptographic schemes. If successful, most of the world's networks should transition to security which will appear seamless to the wider public.

In the end, Y2K wasn't the catastrophe that many doomsayers predicted. Hopefully quantum computers vs public key encryption passes with as little impact as Y2K did.

The moral of the story is that it's important not to ignore the threat posed by a QC. If the NSA is taking steps to secure its networks, then others should take the threat seriously too.

Cryptocurrencies face an existential threat

Quantum computers present an existential threat to many cryptocurrencies. Bitcoin is the logical example to use. Bitcoin's core protocol relies on Elliptic Curve Digital Signature Algorithm (ECDSA) to create a private key and a corresponding public key. A sufficiently powerful QC can derive the private key from the public key. This allows an attacker to access that particular wallet. ECDSA is not easy to crack, but the potential is there and ignoring it is fraught with danger given the notoriously slow pace of blockchain development combined with head-in-the-sand tribalism.

Bitcoin's early wallets are particularly vulnerable due to their use of pay to public key (p2pk) addresses, including the Satoshi Nakamoto era wallets. QC sceptics will say that BTC developers can hard fork to a quantum resistant signature scheme, and that's certainly true, but those dormant wallets remain vulnerable. Some estimates put the number of lost bitcoins at up to 25% of the entire supply. That's a lot of BTC.

What if a million bitcoins suddenly appeared on the market? Confidence would plummet and the price of bitcoin would crash. A hundred billion dollars, give or take is a juicy target for a rogue state. North Korea could certainly use the money.

But BTC and other cryptos aren't just about wealth. Their decentralised nature is antithetical to the ideologies and financial sectors of many countries. A country like China might wish to destroy all confidence in crypto, in order to remain in control of its financial sector. Perhaps the US might covertly attack crypto in order to prevent its use by criminals. Russia might.. well, who knows what Russia might do.

Some cryptos have already adopted QC secure signature schemes. Others including Ethereum and Cardano have quantum signatures or protection on their roadmaps.

I want to note again, my aim here isn't to pronounce doom and gloom. Bitcoin and others will survive if they take steps to protect against QCs, it's just that time is definitely ticking along. Cryptocurrencies already face numerous adversaries day after day, and yet it survives.

But it's time to get past the FUD and take quantum computers seriously. Developers need to act now. It might be a year or 10, but If a black swan event occurs, it'll be far too late to do anything about it. The later the threat gets taken seriously, the harder it will be to mitigate against it.

Do you need to worry about quantum computers?

No. Don't stress. Most of the legwork is being done behind the scenes and your current passwords and data should remain unaffected as long as the corporate caretakers of it are competent.

You can do things like change your private keys to longer key lengths where possible, but it's pretty safe to say that an adversary with a quantum computer isn't going to be worried about accessing your personal router, banking, or Coinbase password. There's bigger fish in the sea to go after.

The main thing is to be aware of the possible threat. The more people that are aware, the more questions get asked and hopefully answered. With any luck, by the time a fully functional quantum computer sees the light of day, the world will continue just as it always has, while enjoying the benefits they will bring.

In the future, hopefully stories like this one will be long forgotten, much like those Y2K doom and gloom articles were. I want to move on to talk about how a quantum computer can help to solve the really big problems, like clean energy, cures or treatments for things like cancer or diabetes, developing next generation materials, climate simulation or managing an entire city full of self-driving cars. But we all know that the likes of China and the US are after strategic and national security objectives first. And with that in mind, the wider internet and cryptocurrency remains vulnerable.

10.Danish Researcher Explains Zero-Knowledge Proofs and Post-Quantum Encryption

by Pat Brans

https://www.computerweekly.com/news/252516064/Danish-researcher-explains-zero-knowledge-proofs-and-post-quantum-encryption

A native of Denmark, Jens Groth became interested in cryptography as a student at the University of Aarhus, where he obtained a master's degree in mathematics and a PhD in computer science – specifically in cryptography. From there, he went to the University of California, Los Angeles (UCLA), where he took a postdoc that revolutionised "zero-knowledge proofs" – a technology that has become very

important in blockchains.

Groth has been working on zero-knowledge proofs ever since, making more major contributions along the way.

A zero-knowledge proof is a protocol between two parties – a "prover" and a "verifier". Through an interaction, the prover demonstrates to the verifier that something is true but doesn't reveal any specific information about why it is true.

"This idea goes back to the 1980s," says Groth. "Computer scientists were looking at the concept of mathematical proofs and noticed the magical fact that you don't actually have to give information beyond the fact that something is true.

"In my research, I introduced some new techniques for building zero-knowledge proofs in a more efficient manner, allowing the proofs to be extremely compact. You can have a huge, complicated statement that takes up gigabytes of space and you can prove that it's correct with just a few hundred bytes. That is super compact."

Groth adds: "I got into this area when I was doing my PhD and was looking at voting protocols. There you have voters encrypt their votes, so nobody else sees what their vote was. There are some tallying mechanisms, so you can aggregate a lot of encrypted votes and get out the right results without looking inside each individual ciphertext.

But those aggregation methods mess up if voters input invalid votes. For example, you could have somebody input minus 1,000 votes for Alice in their ciphertext. It turns out that you can use zero-knowledge proofs to prove that the ciphertext you're sending contains a correct vote – that it's one of the eligible options – without indicating which of those options it is."

These same protocols can be used in many other ways. They could allow a user to show that they fall within a certain age range, without having to reveal exactly how old they are. Users could also prove they have sufficient income to obtain a loan, without having to disclose the exact income or the sources.

Groth describes zero-knowledge as a "Swiss Army knife" for assurance. When a computer runs a protocol, you can use a zero-knowledge proof to ensure it is doing so correctly and without deviation from the protocol. And this assurance comes with total privacy – the zero-knowledge proofs do not reveal confidential data that the computer holds.

The remaining challenge is to make the zero-knowledge proofs efficient enough that they do not cause an unacceptable slowdown. Groth's inventions have drastically reduced this cost – and have inspired more research. Finding further efficiency improvements is now a very active area of research.

The Internet Computer

Groth has transitioned from academia to industry and now applies his expertise to the Internet Computer, which was founded on the idea of having a distributed computer platform that never shuts

down. The idea is that just like you have a shared internet, you can have shared computing services that everyone can access, and developers can build upon. The intention is to protect not only against technical failures and attacks, but also against corporate control, through decentralised governance.

All computation is replicated on multiple computers running in different datacentres around the world, so even if one of them breaks down, or gets hacked, the Internet Computer still runs.

Groth is director of research at DFINITY, a not-for-profit organisation based in Zurich that built and launched the Internet Computer. The platform is open source and DFINITY is currently its biggest contributor. The long-term vision is to grow a large community around the Internet Computer, with DFINITY being only one of many contributors.

The Internet Computer uses blockchain technology to allow machines around the world to come to an agreement about the order in which they execute inputs. Getting agreement among machines comes with a cost, however.

"For any blockchain, it is expensive to write to the blockchain," says Groth. "Every time you do a write, all the machines have to be updated in exactly the same way. They have to reach a consensus on what that way is. All the machines talk back and forth and agree on the order in which they want to execute all the incoming messages from thousands of users.

"If one of the machines is down, or cannot connect to another machine, it doesn't get to vote on the order of the messages. The Internet Computer has a mechanism built in to make it resilient to this situation – it requires only a super majority of machines to agree, so if one of the machines is hacked, the rest can continue without it."

One important aspect of the Internet Computer is that it provides general-purpose computation. Developers can create applications on it, using their favourite language. Most people program in Rust or Motoko, which is a special language developed by DFINITY. They compile their code to something called WebAssembly, which is closer to machine code. This allows developers to write an application and deploy it around the world. By doing this on the Internet Computer, the application is executed with guaranteed security.

The Internet Computer is expected to be a major enabler of Web3, the next iteration of the World Wide Web, which will be highly decentralised and powered by blockchain technologies. Futurists speculate that this decentralised version of the Web would reduce the reliance on major technology players, such as Google and Facebook, and more cooperative business models could be developed with less reliance on advertising revenue.

Web3 would also lead to decentralised finance, allowing users to exchange currency in the form of tokens, without involving banks or governments.

But such a big overhaul is not expected in the current decade. This means that by the time Web3, or some variant, becomes dominant, quantum computing may have become practical. If that is the case, a whole new set of security concerns will have to be addressed.

Post-quantum security

"We have known for a long time that quantum computers will be able to break some of the cryptography we use today," says Groth. "Not all cryptographic algorithms will be susceptible to quantum attacks, but some of the most popular will. Anything based on either the discrete logarithm problem or the factorisation problem needs to be changed.

"Quantum computing is not at the point where we can break key cryptography as it is deployed today on the internet. We don't know exactly how long that is going to take, but it's definitely on the horizon, and we need to prepare for it now because it takes a long time to develop and deploy the cryptography that we will need to protect against quantum computers."

Groth adds: "There is a distinction to be made in the cryptography we use to check things and the cryptography we use to store or exchange information. For instance, if I create a digital signature on a document, send it to you and you check it right now, we don't have to worry because quantum computers are not at a state where they can forge the digital signatures commonly used.

"However, when information is stored or exchanged in encrypted messages, it is important to think about post-quantum cryptography right now. An attacker could intercept a message and save it for five or 10 years, then use a quantum computer to decrypt it.

"Secure multi-party computation is an example of something that requires post-quantum protection. Its goal is to facilitate computation with privacy. In order to keep confidential information private, you have to encrypt the data. You also have this storage problem. If a hacker takes and stores all the communication for a few years – until quantum computers become real – then when they get access to a quantum computer, they can decrypt the information they have stored."

Groth notes that organisations such as the National Security Agency in the US are already storing encrypted information that they might decrypt later when quantum computing can break the cypher. Intelligence agencies in other countries around the world are certainly doing the same.

Fortunately, the cryptographic community is waking up to this concern. The National Institute of Standards and Technology has been organising competitions for researchers to standardise new cryptographic protocols that are secure against quantum attackers.

"We are definitely interested in post-quantum security at DFINITY," says Groth. "Currently, our cryptography relies on the discrete logarithm problem. This works well now, but in the long run it would jeopardise the Internet Computer. Take, for instance, our digital signatures. We use them to certify all data that is coming from the Internet Computer. If you had a quantum computer right now, you could just go and impersonate somebody.

"We need to find a replacement technology for that. We don't need to implement it right now, but we would need to have it ready before quantum computers become a real thing."

Post-quantum security is critical for the future not only of the Internet Computer, but also for blockchain in general, banking transactions, and a lot more. In many cases, the Internet Computer re-

lies on standard protocols that are in widespread use. For example, digital signatures and transport layer security (TLS) are both used.

Groth does not expect to have to work much on these standard protocols, because the wider cryptographic community is already working to standardise post-quantum digital signatures and TLS. The task of people working on the Internet Computer will just be to find the best one of those tools and implement it. The challenge is in the advanced solution that the Internet Computer uses.

"Not only do we have to tweak our protocols to use some of the post-quantum security solutions being developed, but we also have to come up with some tools ourselves," says Groth. "There are areas, sophisticated special-purpose solutions, where we cannot expect the community to solve problems for us. We want to keep the same functionality and security for the Internet Computer without being vulnerable to quantum attacks. There is a lot of research to do on that.

"And then there's a final thing, which is cryptography that we don't have yet, but also needs to be post-quantum secure. One of the research projects we have is to build in confidentiality on the Internet Computer. We want to be able to encrypt the data that the Internet Computer holds. We may want to compute on encrypted data such that nobody can learn what's going on. We want a trusted runtime environment."

Groth adds: "There are different approaches. One is that you could have a trusted execution environment ,which is basically you trust that the chip has a trusted execution environment. The idea is that if you tamper with it, it will break. The problem is that it's hard to rely on hardware because there have been quite a lot of attacks in these trusted execution environments.

"If you're shipping hardware and you find a bug later, it's hard to replace. An alternative approach is secure multi-party computation, which relies on cryptography to protect confidentiality. But this relies very much on encryption and so needs to be post-quantum secure."

The changing role of trust

Breakthroughs in cyber security, such as the invention of public-key cryptography, have enabled internet commerce, where two or more parties who have never met and will never meet are able to establish a secure link and exchange money. With increasing decentralisation and more reliance on peer-to-peer exchanges, cyber security is likely to become even more important in the coming decades.

Economies are becoming increasingly dependent on electronic exchanges, and banks and governments no longer have the control they had before. At first glance, you might assume more trust is required. But, thanks to researchers like Jens Groth, the need for trust has diminished – computer systems can be made to cooperate without reliance on a central party.

11.LG Uplus Launches Commercial Service

# of Quantum-Resistant Cryptography

by Lim Chang-won
https://www.ajudaily.com/view/20220421125518862

LG Uplus has launched South Korea's first commercial service of quantum-resistant cryptography that can defend against hacking attacks on quantum computers. The mobile carrier would discover customized application services for each customer group and expand them to various fields.

LG Uplus (LGU+), a mobile carrier in South Korea, said it would apply quantum-resistant cryptography technology to wired and wireless communication through technology advancement.

As different passwords are used for all IT-related hardware and software with many companies storing and processing numerous big data, a system to prevent the risk of hacking is important. LGU+ said its quantum-resistant cryptography technology will provide an optimal network for customers who require security services that can safely protect data from external threats.

"As a leader in quantum-resistant cryptography technology, LG Uplus will create a technological environment and an industrial ecosystem, which are needed to foster the quantum information and communication industry as a core industry of the country," Koo Sung-chul in charge of LGU+'s wired network business said in a statement on April 21.

Data encoded in a quantum state is virtually unhackable without quantum keys which are basically random number tables used to decipher encrypted information. Even though current, publicly known, experimental quantum computers lack the processing power to break any real cryptographic algorithm, cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat.

LGU+ has commercialized post-quantum cryptography (PQC) technology, which refers to cryptographic algorithms. PQC does not require separate network infrastructure to distribute cryptographic keys because it can be applied flexibility to different sections of wired and wireless networks that require encryption.

A dedicated PQC line provides an environment that cannot be hacked through a reconfigurable optical add-drop multiplexer (ROADM). It is a method of encrypting and decrypting data with a quantum-resistant encryption key when a customer transmits and receives data through a dedicated line.

12.AMD and Web 3 Firms Launch $7M Contest for Zero-Knowledge Cryptography

by Dean Takahashi
https://phys.org/news/2022-04-chinese-team-distance-quantum.html

We are excited to bring Transform 2022 back in-person July 19 and virtually July 20 - 28. Join AI and data leaders for insightful talks and exciting networking opportunities. Register today!

A coalition of 22 leading zero-knowledge technology companies, foundations, and funds including Advanced Micro Devices, Aleo, Anoma, the Ethereum Foundation, Matter Labs, Mina Protocol, Polkadot Pioneers Prize, and Polygon have launched a contest to advance the technology.

The companies will give away $7 million in the ZPrize contest to accelerate zero-knowledge cryptography, which can make blockchain technology — used in everything from games to crypto art — more efficient and less wasteful when it comes to computing power and transactions.

The contest is modeled after the famous XPrize competitions that have used private contributions to fuel advances in a variety of areas including spaceflight, adult literacy, and ocean health. For the ZPrize, teams will compete for awards by engineering new algorithms and techniques that achieve performance metrics unmatched by the best zero-knowledge systems deployed in the blockchain industry today.

One of the most promising approaches for scaling zero-knowledge technology is to use specialized hardware like graphics processing units (GPUs) or field-programmable gate arrays (FPGAs). So ZPrize is collaborating with AMD-Xilinx to provide access to cutting-edge hardware such as the Varium C1100 blockchain accelerator card for competing teams to develop the best solutions to the ZPrize challenges.

"Incorporating zero-knowledge cryptography in a blockchain platform is critical for widespread adoption of the technology, but it comes with a significantly increased compute workload," said Hamid Salehi, director of product marketing at the AECG Data Center Group at AMD, in a statement. "FPGAs are uniquely positioned to accelerate the zero-knowledge protocol efficiently, at the hardware level, to create scalable blockchain solutions. AMD-Xilinx is proud to support the ZPrize competition with our FPGA-based accelerators to enable the community to create innovative solutions that help advance zero-knowledge technology."

Zero knowledge proofs

As blockchain technology and Web3 expand into more use cases, it faces the challenge of scaling to hundreds of millions of users while at the same time remaining trustless, secure, and accessible. Zero-knowledge is a new technology that shows great promise in solving these problems. Since its introduction by ZCash in 2016, the technology has evolved through rapid-fire innovation. That's why industry and academic experts alike view it as the key to enabling mainstream adoption of Web3 and blockchain technology.

To understand the significance of zero-knowledge proofs, you need a basic understanding of

blockchain, the transparent and secure digital ledger which uses a network of computers to verify the truth of a piece of data on one computer. If the distributed and immutable ledger confirms that the data is the same across that network, then that data is verified.

Blockchains such as Ethereum have become popular for hosting blockchain games with nonfungible tokens (NFTs), which use blockchain to authenticate unique digital items in games. But those blockchains can consume a lot of energy when they use the network to verify every little detail in a game, like who beat a boss or won a match.

It's a form of cryptography that allows for basically verifiable computations. What that means is that an application runs a piece of code and you offer a proof that this result came from that code. That magic basically lets you shortcut and fast track a ton of steps that you otherwise would have the network run for you.

By doing this, a game can utilize the company's own servers for doing things like crafting of in-game items, rather than running that on the blockchain in a way that consumes a lot of energy and costs. Wu said you can take take a complex logic, like fighting a boss and play out that entire battle between your character and boss — but do it off the blockchain, rather than on it. That uses a lot less computing power and energy, but it could be less secure.

The game company can create a full log, or a full transcript of what happened during that entire process, and just give the final outcome along with the proof. The proof is sent on the blockchain and the network that verifies transactions on the blockchain can verify the proof. If it mathematically checks out, then it concludes that you really played this battle with the boss. That is, it can verify the accuracy of the data without activating the blockchain network's host of computers.

Then the game company can circumvent replaying the entire set of events that happened and just accept the final outcome on the network. The partners send that proof to the network with the final outcomes so that it can then be recorded onto the blockchain. Aleo is building its own Layer 1 blockchain to host this type of technology, similar to others like Dapper Labs with its Flow blockchain. But Aleo is also implementing a multi-chain ecosystem.

The ZPrize challenge

Teams will compete to win financial rewards in both dollars and tokens across a range of categories that the sponsors have identified to be of particular importance for practical application of zero-knowledge systems. Submissions will be judged against the existing technical benchmarks, with the highest rewards paid out for the greatest improvements on the current state-of-the-art.

"Espresso Systems is proud to sponsor the ZPrize, an industry-wide collaboration which we believe will be crucial to advancing zero-knowledge as a technology," said Jill Gunter, chief strategy officer for Espresso Systems, in a statement. "Zero-knowledge systems are paving the way toward mass adoption of decentralized applications as they transform the way we interact and transact online and the ZPrize is an important effort to accelerate that progress."

The cooperation of competing entities embodied by ZPrize centers around the shared objective of

making widespread application of this technology practical and enabling privacy and scalability in web 3. To that end, winners of the competition must open-source their challenge solutions so that the entire community can access and benefit from them fully.

"The goal of the ZPrize is to spur a quantum leap in zero-knowledge cryptography that so many Web3 protocol and application developers are waiting for to enable their products to scale to millions," said Alex Pruden, chief operating officer of Aleo and founder of the ZPrize initiative, in a statement. "The sponsors of ZPrize not only represent an industry but a united community of believers in this technology. We share a collective desire to turn these exciting academic ideas into a deployed reality. With the ZPrize, we're advancing the state-of-the-art to form the bricks of the technological foundation that will scale and secure the next-generation web."

ZPrize sponsors include, in alphabetical order, 0xPARC, Aleo, Algorand, Anoma, Aztec Protocol, Celo, CoreWeave, DZK, Espresso Systems, Ethereum Foundation, Findora, Harmony One, Kora, Manta Network, Mina Protocol, Matter Labs, the Polkadot Pioneers Prize, Polychain Capital, Polygon, RISC0, Trapdoor Tech, Zero Knowledge Validator

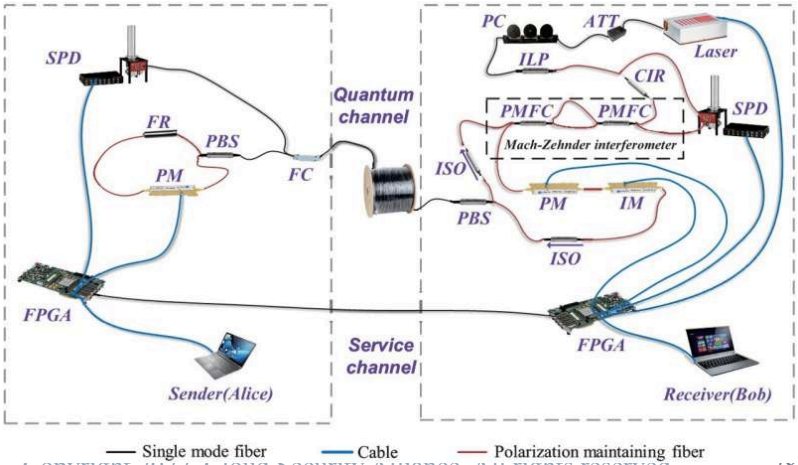
Anyone with academic or industry experience in mathematics, cryptography, electrical engineering, hardware engineering, or optimization is encouraged to apply.

13.Chinese Team Breaks Distance Record For Quantum Secure Direct Communication

by Bob Yirka

https://phys.org/news/2022-04-chinese-team-distance-quantum.html

A team of researchers at Tsinghua University in China, has broken the distance record for quantum secure direct communication (QSDC) by sending information using their protocol a distance of 102.2 km. In their paper published in the journal Light: Science and Applications, the group describes how they devised a new QSDC protocol and used it to send secure signals over a fiber cable to extend the distance such messages could be sent.



Laser: 1550 nm with pulse-repetition frequency 50 MHz; FPGA field programmable gate array, ATT attenuator, PC polarization controller, ILP in-line polarizer, CIR optical circulator, PBS polarization beam splitter, FC 90:10 filter coupler, PMFC polarization maintaining filter coupler, PM phase modulator, IM intensity modulator with extinction ratio of 45.1 dB, ISO isolator, FR 90 degree Faraday rotator, SPD superconducting nanowire single-photon detector with over 85% detection efficiency, 50 Hz dark count rate and 15 ns reset time. The asymmetric Mach–Zehnder interferometer consists of two PMFC, and the delay length is about 2 m

QSDC takes advantage of entanglement as a means of securing network transmission over unsecured data lines. Because such particles are linked in a way that cannot be changed, protocols using them cannot be hacked without being detected by systems on the intended receiving end of such messages. As research has progressed to allow for the use of QSDC in real-world applications, the goal has been to reduce errors, increase transmission rates and, above all, extend the distance that messages using the protocol can be sent. Prior to this new effort, the record was just 18 km.

To extend that distance, the researchers devised a new QSDC protocol, one that involves the use of photonic time-bin states for monitoring signals and phase states for the actual communication messages. The researchers suggest adding such features to the QSDC protocol protects against phase errors and polarization. Further, it does not rely on feedback nor accurate matching of pairs of interferometers. They also suggest it makes such systems more reliable as well, which in turns leads to a lower error rate. And lowering the error-rate allows for extending the distance messages using the protocol can be sent.

The researchers acknowledge that the transmission rate is slow, at just 0.54 bps, which is slower even than systems using classical computing. But they note that it is still fast enough to allow for sending encrypted messages or even phone calls. They suggest their work shows that it is possible to create intercity QSDC-based networks using current technology. And they further suggest that certain parts of the Internet now in place could be replaced with parts based on the QSDC protocol they have developed to allow for hacker-resistant communications.

14.Space-Efficient Binary Optimization For Variational Quantum Computing

by Karine
https://thequantumhubs.com/space-efficient-binary-optimization-for-variational-quantum-computing/

In the era of Noisy Intermediate-Scale Quantum (NISQ) computers it is crucial to design quantum algorithms which do not require many qubits or deep circuits. Unfortunately, most of the well-known quantum algorithms are too demanding to be run on currently available quantum devices.

Moreover, even the state-of-the-art algorithms developed for the NISQ era often suffer from high space complexity requirements for particular problem classes.

Researchers have showed that it is possible to greatly reduce the number of qubits needed for the Travelling Salesman Problem (TSP), a paradigmatic optimization task, at the cost of having deeper variational circuits.

While the focus is on this particular problem, they claim that the approach can be generalized for other problems where the standard bit-encoding is highly inefficient.

The team also proposes encoding schemes which smoothly interpolate between the qubit-efficient and the circuit depth-efficient models. All the proposed encodings have the same volume up to polylogarithmic factors and remain efficient to implement within the Quantum Approximate Optimization Algorithm framework.

15.The Case for Implementing Post-Quantum Cryptography Today

by Rebecca Krauthamer
https://solutionsreview.com/security-information-event-management/the-case-for-implementing-post-quantum-cryptography-today/

Public-key cryptography has become an indispensable component of our global communication digital infrastructure in the past three decades. This technology keeps our data safe and scrambles data by plugging one number into an encryption algorithm, which then descrambles the data when another number is introduced. The former is the "public key," and the latter is the "private key." Large-number factoring is the foundation of today's encryption standards powering public-key encryption. It is mathematically impossible to reverse engineer a private key with a "brute force" calculation on today's computers.

At least, that's what it looks like today, but powerful quantum computers will emerge on the near horizon (as soon as three years) that will change things. Quantum computers can slice through data like no computer can today and breakthrough code causing massive data breaches. Classical computers use digital bits to process data as zeros and ones. These computers are typically set for general or special purposes, programmed to perform various tasks. Quantum computers use qubits, which can simultaneously represent any combination of zeros and ones. The logic of a quantum computer offers possibilities beyond that of a traditional computer because it does not have to reduce data to a string of zeros and ones by using sub-atomic properties like superposition and entanglement.

These mega computation devices will unlock too many valuable opportunities to count. And they are also incredibly good at solving precisely the kind of math that has kept public key encryption unbreakable for so many years.

Potential Impacts on Organizations

Imagine a bad actor being able to intercept encrypted enterprise intellectual property, private financial information, personal health data, or sensitive personally identifiable information (PII) that flows across the globe, reading it as quickly as you can read this article. Secrets could be unlocked and

leveraged the way we did after cracking the Nazi Enigma codes.

Banks, government agencies, healthcare organizations, other enterprises, or anyone trusted with sensitive information should think not just about preparing for the future but about the SNDL—store now, decrypt later—scenario happening today. Aaron Moore, Co-Founder of Optimized Talent, said, "The immediate threat is that an attacker can record data encrypted using asymmetric encryption now in preparation for breaking the encryption later, once scalable quantum computing is available. This is particularly threatening for long-lived information assets (think bank account numbers, for example). Post-quantum resilience is needed today."

Even if the ability for quantum computers to decrypt data is several years away, data still has a shelf life. Leading organizations understand people need to be able to trust that their data, private health records, and bank account information need to remain secret today and 5 to 10 years from now.

In 2021, the average cost of a data breach was $4.2 million, but the threat is much more significant in quantum. Last year, the Hudson Institute used an 18,000-point econometric model and found that the first quantum computing breach of a top financial institution in the US could start a cascading financial failure that would cost nearly $2 trillion and impair up to 60 percent of the US financial assets. This result would not be a typical data breach and would mean that a hacker has deployed the capability to break down the number one line of trusted defense: encryption.

Organizations have both a financial and ethical responsibility to protect the sensitive data they are trusted with. It is essential to take the threat seriously, and the fix is available. The good news is that you do not need a quantum computer to stop a quantum attack. Organizations can utilize classical math to eliminate holes exposed by quantum computers. NIST is standardizing a new set of quantum-resilient cryptographic algorithms. These algorithms will be the standard in a post-quantum computing world when made official.

This is not theoretical and is an already defined, necessary upgrade. For example, this past January, the White House issued an executive order to put near-term requirements in place for federal agencies to start a quantum resilient upgrade. The memo states that it is now mandatory for government data to be post-quantum secured.

In March 2021, Secretary of the Department of Homeland Security Alejandro Mayorkas outlined his vision for cybersecurity resilience and identified the transition to post-quantum encryption as a priority. The Department of Homeland Security also released policy guidelines to drive their preparedness efforts. Discussions in previous years were much more fragmented, but the executive order makes things clear. Organizations will soon have to upgrade to post-quantum security technology.

Highly regulated industries like healthcare, pharmaceuticals, finance, critical infrastructure, and energy will soon need to follow suit. It is also crucial for organizations that work closely with the government or provides goods and services to anticipate their requirements to become post-quantum compliant.

But even before NIST's standards and the executive order requirements take effect, there is an opportunity to get ahead of the curve now. A new study from Harvard Business Review (HBR) Analytic

Services-The Digital Dividend – First Mover Advantage outlined how organizations can secure the first-mover advantage in terms of public recognition and trust among customers, clients, and revenue. Historically the revenue growth of early adopters is "more than three times the growth experienced by 'cautious' technology adopters (those that wait until a technology is well-established)."

Post-quantum cyber-attacks are a real threat we must take seriously, and we need to start right away. But it is an entirely solvable problem for organizations with the proper steps in place.

16.British Encryption Startup Arqit Overstates Its Prospects, Former Staff And Others Say

by Byron Tau, Dustin Volz, Eliot Brown

https://www-wsj-com.cdn.ampproject.org/c/s/www.wsj.com/amp/articles/british-encryption-startup-arqit-overstates-its-prospects-former-staff-and-others-say-11650274200

A U.K. cybersecurity startup rocketed to a multibillion-dollar valuation when it listed publicly last fall on the promise of making encryption technology that would protect the defense industry, corporations and consumers alike from the prying eyes of next-generation computer systems. Founder and Chief Executive David Williams told investors at the time that his company, Arqit Quantum Inc., had an "impressive backlog" of revenue and was ready "for hyperscale growth."

But Arqit has given investors an overly optimistic view of its future revenue and the readiness and workability of its signature encryption system, according to former employees and other people familiar with the company, and documents viewed by The Wall Street Journal.

While the company says it has a solution to a quantum-computing security challenge that U.S. intelligence last year said "could be devastating to national security systems and the nation," government cybersecurity experts in the U.S. and the U.K. have cast doubt on the utility of Arqit's system.

Arqit's stock price reached its highest level to date of $38.06 on Nov. 30 and has since fallen to $12.49, including a 17% drop Monday. There has been a broad pullback of young tech stocks.

When the company secured its Nasdaq listing last autumn, its revenue consisted of a handful of government grants and small research contracts, and its signature product was an early-stage prototype unable to encrypt anything in practical use, according to the people. The encryption technology the company hinges on—a system to protect against next-generation quantum computers—might never apply beyond niche uses, numerous people inside and outside the company warned, unless there were a major overhaul of internet protocols.

Arqit disputed that its encryption system was only a prototype at the company's market debut. "This

was a live production software release and not a demonstration or trial," said a company representative. "It was being used by enterprise customers on that day and subsequently for testing and integration purposes, because they need to build Arqit's software into their products."

In Arqit's investor presentation shortly before going public, Mr. Williams said the company's technology can solve the problem of quantum attack "for every connected device in the world and that means that the Arqit business is now suitable for hyperscale growth."

Arqit went public by merging with a special-purpose acquisition company, a process that isn't subject to the rules about disclosure and marketing practices that govern standard initial public offerings. The SPAC process gives companies more freedom to woo investors with projections of future revenue and profit, a dynamic that has helped many companies with no revenue list publicly at multibillion-dollar valuations.

In light of investment-protection concerns, U.S. regulators last month proposed a bevy of new requirements for SPACs. Bankers and other supporters say SPACs provide a crucial path for investors to get into fast-growing companies early.

Arqit's stated aim to future-proof communication systems from the danger of a quantum computer is a top concern for policy makers. Senior U.S. national-security officials in recent years have warned with increasing urgency of a potential national-security calamity if China or another adversary achieves a breakthrough in quantum computing, which relies on quantum bits, or qubits, to represent and store information in a quantum state that is a complex mix of zeros and ones, rather than traditional binary computers that store information as either one or the other.

British cybersecurity officials questioned the viability of Arqit's proposed approach to encryption technology in a high-level evaluation they privately shared with the company in the summer of 2020, according to people familiar with the matter.

Asked about the negative review, a spokesman for Britain's National Cyber Security Centre said the agency "helps companies understand the security properties of their products and systems, including those in the quantum sector. We do this on a case-by-case basis, and in confidence."

Through a spokesman, Arqit said it "has a positive, ongoing relationship with the NCSC" and that the agency hasn't reviewed its current technology.

The U.S. National Security Agency and the NCSC published separate assessments in recent years warning against using satellite-based encryption systems like those Arqit is proposing to integrate into its current product in the next few years. The NSA said its warning was unrelated to any specific vendor, a spokesperson said.

In April 2021, Arqit's chief revenue officer resigned after raising concerns with Mr. Williams that he was overstating contracts and giving unrealistic revenue projections to potential investors, people familiar with the matter said. Several other former employees said they had similar concerns about both the business model and the maturity of the technology, prompting them to also leave since then.

Arqit is building an encryption system designed to protect computer systems from quantum computers, which are forecast to someday be able to break the security on nearly all existing commercial cryptography systems. The company has said its technology would revolutionize computer security and draw customers from major corporations and the defense sector. Several former senior officials with British intelligence agency GCHQ, as well as retired U.S. and U.K. generals, serve on Arqit's board and advisory committees or in management.

Founded by veterans of the satellite industry, Arqit plans to incorporate space-based transmissions as part of its encryption system, coupled with a different way of distributing secure secret encryption keys than current technology does. It launched one part of the encryption product in August without the space-based component, which it says will make the system even more secure when it comes online in 2023.

The encryption system—with or without its satellite components—depends on the broad adoption of new protocols and standards for telecommunications, cloud computing and internet services that currently aren't widely supported, people familiar with the matter said.

Steve Weis, a San Francisco-based cryptographer and entrepreneur, said that what Arqit was proposing—relying in part on transmitting quantum information from satellites—is a well-known 1980s-era technology with limited real-world application. "There have been many proofs of concept and companies trying to sell products," he said. "The issue is that there is no practical-use case."

Some senior U.S. national-security officials have reached similar conclusions. The technology, which is called Quantum Key Distribution, has been the subject of study and debate within the national-security world for decades. "QKD is a wonderful quantum-physics demonstration and elements of it have potential long-term implications for various technologies," a senior U.S. defense official said. "That said, widespread adoption of QKD would likely require a physical rebuild of the internet to be effective."

Arqit said it "does not, and never has, supplied QKD technology" and instead has invented a new quantum protocol that solves problems presented by previous iterations of the technology and combines that with a different way of delivering encryption services. The company said it has made improvements on 1980s-era QKD protocols and is building a system that is fundamentally different from earlier generations of the technology.

Beyond the technological concerns, Arqit's revenue and profit projections have come under fire.

When the company announced its SPAC merger in May 2021, a month after the chief revenue officer resigned, it publicly released forecasts that the startup would rapidly become highly profitable, projecting $660 million in revenue in 2025, from which the company expected $447 million in earnings before costs such as depreciation and taxes.

Key to the company's pitch was its claim that it had a large stream of future revenue locked in as the product was live and already selling well. "Customers are using the Arqit products today—and they are universally finding it to be an important part of their technology future," Mr. Williams said in an August investor presentation shortly before the merger closed. He added, "The Quantum Cloud product is live for service and we already have $130 million in signed committed revenue contracts."

"These are contracts where the revenues will definitely be delivered," the CEO said.

The people familiar with the matter said that the bulk of the company's committed revenue isn't from selling its product and that at its public launch, the company had little more than an early-stage prototype of its encryption system. Several clients the company lists—including a number of British government agencies—are simply giving Arqit research grants, nonbinding memorandums of understanding or research agreements that come with no funding, not contracts for its encryption product, they said.

No commercial customer was using Arqit's encryption system with live data when it made its market debut in September, the people said, and the system couldn't meaningfully use any of the common internet protocols required to do nearly anything online. They said it has signed two master distribution agreements with BT Group PLC and Sumitomo Corp. for the still-unrealized satellite component of its technology that are cancelable under certain conditions.

Through a spokesman, BT declined to comment on what it said were "private contractual agreements." Sumitomo declined to comment, citing a nondisclosure agreement.

Arqit defended the maturity of its technology and said its master distribution agreements contained guaranteed revenue. It declined to discuss specifics. Charles Palmer, a spokesman for Arqit, said it was "incorrect and misleading" to say Arqit's major contracts were cancelable.

In securities filings, Arqit was less definitive about its future revenue: It said its customer contracts are contingent upon the "successful delivery of operational technology, which is still under development," and that some contracts depended on successfully completing pilot programs with customers.

Inside the company, Mr. Williams was frequently an abrasive and volatile presence, former employees said, presenting an additional factor alongside doubts about the product for many who have left the company. The former head of human resources, Jane Bashford-Hobbs, has filed a formal complaint with a British tribunal alleging that Mr. Williams bullied employees and that Arqit discriminates on gender in its compensation. Arqit and Mr. Williams didn't respond to requests for comment on the complaint, which remains under seal.

When Britain's NCSC unfavorably evaluated the company's proposed technology nearly two years ago, Mr. Williams was apoplectic, according to people who worked for Arqit at the time. He convened a virtual company meeting in which he dismissed the letter and referred to Ian Levy, the British cyber agency's technical director, as a "f— Jewish c—," the people said. (Mr. Levy isn't Jewish, according to people who know him.) Mr. Williams continued to denigrate Mr. Levy and the NCSC for weeks after the rebuke, some of the employees said.

Employees who witnessed Mr. Williams's reaction were concerned that the incident showed an inability to respond constructively to legitimate feedback, blunting the company's prospects, people familiar with the matter said.

17.How Much Money Has China Already Invested into Quantum Technology?

by Amara Graps
https://quantumcomputingreport.com/how-much-money-has-china-already-invested-into-quantum-technology/

It is hard to estimate how much the Chinese government has already invested in quantum technology, but here is an attempt to provide a best estimate using verifiability and open sources as materials.

The Sleuthing Strategy:

1) A China quantum expert foundation +
2) top-down : China policy interests +
3) bottom up: implementations.

The foundation: 1) an insider's view: report by Chinese quantum workers: "Quantum Information Science" by Qiang Zhang, FeihuXu, LiLi, Nai-Le Liu and Jian-Wei Pan, 2019, and 2) a broad, objective analysis:"Quantum Hegemony" by Elsa B. Kania & John K. Costello, published in 2018. With this foundation, I have filled in the gaps, especially in recent years.

Quantum Research and Technology Projects

Chinese quantum technology funded subjects include quantum information research, quantum control, quantum sensing, quantum materials, quantum dots, quantum cryptography, quantum chips, plus the quantum communication that China is actively advancing.

Quantum Communication

Of the latter, China's most visible quantum technology implementations are their Quantum Secure communication Networks -- regional "Trunks" — combined with their quantum satellite project (nicknamed Micius or Mozi (Chinese: 墨子).

Quantum Research

China's National Natural Sciences Foundation, and the Chinese Academy of Sciences (CAS) provide the funding for many of the other quantum technology areas. Additionally, CAS and the University of Science and Technology of China, with support from institutes all over China, are building a new National Laboratory for Quantum Information Science, aimed to become the world's largest quantum research facility. Construction is underway with reportedly 1600 construction workers. To help you sort out the name: Chinese social media refers to the new laboratory as 'CAS Center for Excellence on Quantum Information and Quantum Physics', seen here with Research Building #1 nearly completed in Hefei in

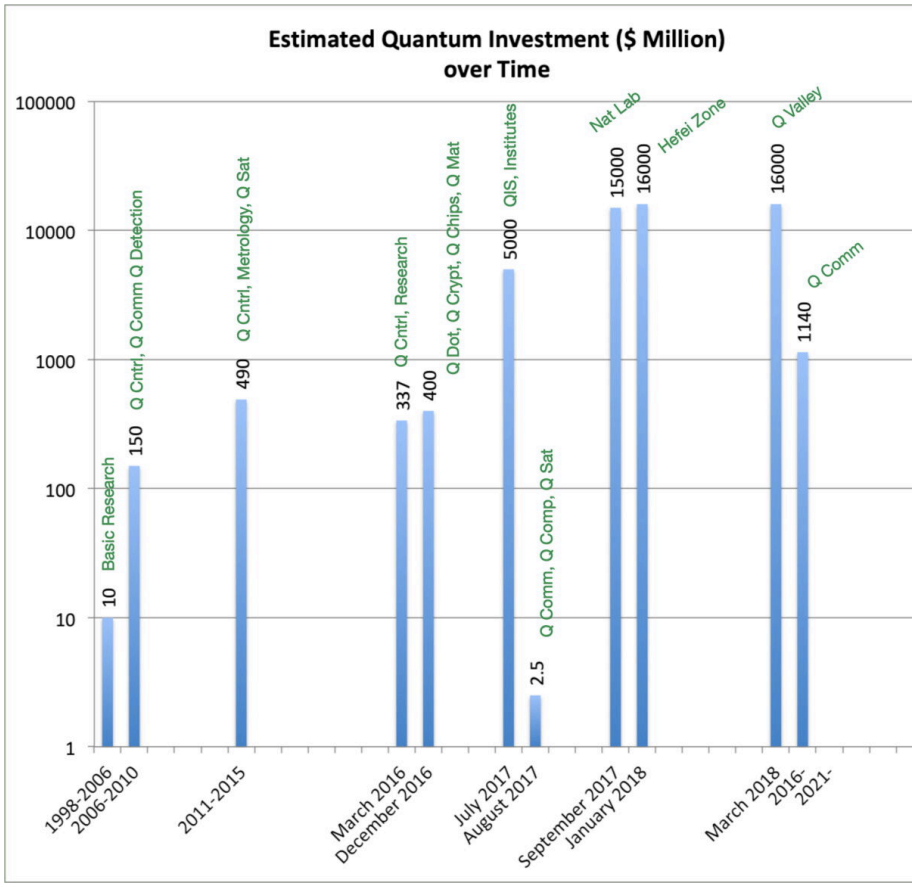
March 2021. If you are wondering about the building's odd shape, it is to pay tribute to Albert Einstein's light-quantum equation $E = hv$.

Funding for an additional broader purpose quantum organization: the Quantum Information and Quantum Science and Technology Innovation Research Institute or Quantum Innovation Research Institute for short, is aimed to support the above National Laboratory, while also developing the growth of quantum industries in Hefei and beyond.

Investment Sum, So Far

The sum of their investment to 2018 is at least $5 billion, possibly reaching $10 billion with the communication networks including the quantum satellites. Added to that figure is $15 billion through approximately 2022, for the National Laboratory for Quantum Information Science with the overarching Quantum Innovation Research Institute.

Therefore, it is estimated that there has been at least a $25 billion Chinese government investment from the mid-1980s through 2022 into quantum technology without including private investment and funding under the current 'Five Year Plan' (FYP).



Why is the Chinese Government Investing World Record Quantities in

Quantum Technology?

China's Quantum Technology Policy Interests

Kania and Costello suggest that quantum technology serves a dual-use purpose to "offset" key pillars of U.S. military power, potentially undermining critical technological advantages.

It was in 2013, when the international security experts read the leaks of former NSA contractor Edward Snowden, which revealed the extent of U.S. intelligence capabilities and activities in China. According to Pan Jian-Wei, this event greatly increased both China's national cyber security activities and raised the urgency of his work.

According to the Canadian Security Intelligence Service, China has emerged as a clear leader in research and development in quantum cryptography, while constructing a national quantum communications infrastructure that could better protect, sensitive military and government communications against potential adversaries' signals intelligence and cyber-espionage capabilities. China's new National Laboratory for Quantum Information Science, when it is completed, will reportedly engage in research "of immediate use" to China's armed forces.

In addition, quantum technology fits neatly into the government's every five year plan, in whichever theme, it has adopted for that time period. The Chinese government's 2016 National Key Research and Development Plan, which specifically describes quantum technology as one of its pillars, streamlines the investments.

Quantum Technology in China's Five-Year Plans

China's Five-Year Plan is the country's quinquennial strategy for economic development: a time segment with a national theme, growth targets, evaluations and new reforms. The First Plan was in 1953–1957. The 14th Five-Year Plan (2021-2025) is now. To show how wide and deep China's support for quantum technology is, here are China's current main stakeholders:

- Ministry of Science and Technology (MOST)
- Ministry of Industry and Information Technology (MIIT)
- National Development and Reform Commission (NDRC)
- National Natural Science Foundation of China (NSFC) –managed by MOST
- Chinese Academy of Sciences (CAS)
- Ministry of Finance (MOF)
- Ministry of Defense (MOD)
- Ministry of Education (MOE)
- Industrial and Commercial Bank of China
- China Construction Bank
- China Internet Investment Fund
- China Reform Fund
- All Provincial and Municipal governments

Early in the 13th 'Five Year Plan' (2016-2020), MOST launched the 'Quantum Control and Quantum Information' National Key Research and Development (R&D) project, more than $100 Million investment, which had a similar effect to the Snowden leaks – Chinese quantum development was accelerated once again. Since MOST is a rare Chinese Ministry that puts its budget transparently on its website, it's worth to note that its year budget is on the order of $80 billion per year.

The 'Targets table' on page 45 of the 2020 final budget is especially intriguing. In this country's large capacity for planning and documenting everything, is a point system incentive for managers to track employees' papers and patents to meet China's targets. Their Targets table carries the line: "Provide method support for breaking through foreign patent blockade, breaking technology monopoly..." This line item would be one of the drivers for the country's large number quantum patents.

18.China Claims 'World Record' in Quantum Communications (QSDC); Says Securely Transmitted Data Over 100 Km

by Ashish Dangwal
https://eurasiantimes.com/china-claims-world-record-in-quantum-communications/

Beijing's ambition to revolutionize quantum communication looks to be succeeding, as Chinese scientists claim to have set a world record for the longest quantum secure direct communication (QSDC), transferring information securely over 100 Km (62 miles)

Long Guilu, the developer of quantum-based secure direct communication technology, and his team announced that they have achieved a new distance record by safely transmitting data over 100 Km (62 miles), reported SCMP.

The observations were published in the journal Light: Science & Applications in early April in an article titled "Realization of quantum secure direct communication over 100 Km fiber with time-bin and phase quantum states."

Despite transmission speeds being slow (0.54 bits per second), the paper noted that it was a major improvement over Long's previous record of 18.5 Km set in 2020, two decades after he devised the device that can identify and prevent eavesdropping threats.

Long, a Tsinghua University physics professor and vice-president of the Beijing Academy of Quantum Information Sciences, noted the transmission speeds, saying they were good enough for phone calls and text messaging at roughly 30 Km.

He claimed that the technology was ready to be integrated with standard encryption techniques to create a secure network with classical relay points.

"If we replace parts of the internet today, where more eavesdropping attacks happen, with quantum channels, those parts will have the added ability to sense and prevent eavesdropping, making communication even safer," Long added.

A bank account password, for example, could be securely communicated between two devices 90 Km away using three 30 Km quantum channels connected by two relay points and protected by encryption, according to Long.

The most notable aspect is that any eavesdropping attempt during quantum transmission would be spotted, whereas information at the relay points would be safeguarded by classical encryption.

"The experiment shows that intercity quantum secure direct communication through the fiber is feasible with present-day technology," the team noted, adding that the technique also has "great potential" to secure the 6G technology.

The longest QSDC distance published before this breakthrough was 18.5 Km. "The rapid progress of quantum computing causes anxiety over the security of those traditional communications," the Chinese quantum team wrote.

China's Quantum Communication Advances

China has made strides in quantum technology's industrial utilization. In recent years, it has made several quantum technological advances, such as the world's first quantum satellite, a 2,000 Km quantum communication line between Beijing and Shanghai, and the world's first optical quantum computing machine prototype.

Additionally, one of Beijing's aims for its 14th five-year plan, which ends in 2025, is to establish an intercity quantum demonstration network based on secure relays. In November of last year, the goal was also incorporated into the city's international science and technology innovation center team the construction plans.

Although it's unknown how much further Chinese researchers have progressed in quantum computing, the Pentagon's 2021 report to Congress on China states that China "continues its pursuit of leadership in key technologies with significant military potential."

According to the science journal Nature, the University of Science and Technology of China in Hefei conducted the first "definitive demonstration" of using quantum mechanics for computations that would be "prohibitively slow on classical computers" in 2020.

While there have been no reports of it being used for military purposes, experts believe the technology could be used in the future by China's armed forces. Quantum could help detect submarines and stealth aircraft among other "military vehicles," said Heather West, a senior research analyst with market research firm IDC in the US state of Massachusetts. Quantum computing can break "classical algorithms" to check on another country's military, she told VOA.

China has already concerned other countries by combining civilian and military assets as part of a Military-Civil Fusion Development Strategy, making it difficult for the rest of the world to predict when academic research will become a valuable resource for the People's Liberation Army.

Meanwhile, other countries are working on this arena as well. Quantum computing is included in the AUKUS military technology sharing agreement between Australia, the United Kingdom, and the United States, which was unveiled in September last year.

According to the National Defense Industrial Association, the White House, National Science Foundation, and Department of Energy stated in August 2020 that they would grant $625 million over five years for quantum R&D.

Quantum computing and quantum communication are still in their early stages of development. For many years to come, none of this research will be of practical application. However, quantum technology has significant geopolitical implications: fully functional quantum networks might offer unhackable communication routes, and a potent quantum computer might theoretically overcome most of the encryption used to safeguard emails and Internet operations.

19.Quantum Internet Breakthrough – Bell State Analyzer Presents Giant Leap Toward Fully Quantum Internet

by Oak Ridge National Laboratory
https://scitechdaily.com/quantum-internet-breakthrough-bell-state-analyzer-presents-giant-leap-toward-fully-quantum-internet/

Technologies that harness the power of nature's most minute scale show enormous potential across the scientific spectrum, from computers exponentially more powerful than today's leading systems, sensors capable of detecting elusive dark matter and a virtually unhackable quantum internet.

Researchers at the Department of Energy's Oak Ridge National Laboratory, SRI International, Freedom Photonics and Purdue University have made strides toward a fully quantum internet by designing and demonstrating the first-ever Bell state analyzer for frequency bin coding.

Their findings were published in Optica.

Before information can be sent over a quantum network, it must first be encoded into a quantum state. This information is contained in qubits, or the quantum version of classical computing "bits" used to store information, that become entangled, meaning they reside in a state in which they cannot be described independently of one another.

Entanglement between two qubits is considered maximized when the qubits are said to be in "Bell states."

Measuring these Bell states is critical to performing many of the protocols necessary to perform quantum communication and distribute entanglement across a quantum network. And while these measurements have been done for many years, the team's method represents the first Bell state analyzer developed specifically for frequency bin coding, a quantum communications method that harnesses single photons residing in two different frequencies simultaneously.

"Measuring these Bell states is fundamental to quantum communications," said ORNL research scientist, Wigner Fellow and team member Joseph Lukens. "To achieve things such as teleportation and entanglement swapping, you need a Bell state analyzer."

Teleportation is the act of sending information from one party to another across a significant physical distance, and entanglement swapping refers to the ability to entangle previously unentangled qubit pairs.

"Imagine you have two quantum computers that are connected through a fiber-optic network," Lukens said. "Because of their spatial separation, they can't interact with each other on their own.

"However, suppose they can each be entangled with a single photon locally. By sending these two photons down optical fiber and then performing a Bell state measurement on them where they meet, the end result will be that the two distant quantum computers are now entangled — even though they never interacted. This so-called entanglement swapping is a critical capability for building complex quantum networks."

While there are four total Bell states, the analyzer can only distinguish between two at any given time. But that's fine, as measuring the other two states would require adding immense complexity that is so far unnecessary.

The analyzer was designed with simulations and has demonstrated 98% fidelity; the remaining 2% error rate is the result of unavoidable noise from the random preparation of the test photons, and not the analyzer itself, said Lukens. This incredible accuracy enables the fundamental communication protocols necessary for frequency bins, a previous focus of Lukens' research.

In the fall of 2020, Lukens and colleagues at Purdue first showed how single frequency-bin qubits can be fully controlled as needed to transfer information over a quantum network.

Using a technology developed at ORNL known as a quantum frequency processor, the researchers demonstrated widely applicable quantum gates, or the logical operations necessary for performing quantum communications protocols. In these protocols, researchers need to be able to manipulate photons in a user-defined way, often in response to measurements performed on particles elsewhere in the network.

Whereas the traditional operations used in classical computers and communications technologies, such as AND/OR, operate on digital zeros and ones individually, quantum gates operate on simultaneous su-

perpositions of zeros and ones, keeping the quantum information protected as it passes through, a phenomenon required to realize true quantum networking.

While frequency encoding and entanglement appear in many systems and are naturally compatible with fiber optics, using these phenomena to perform data manipulation and processing operations has traditionally proven difficult.

With the Bell state analyzer completed, Lukens and colleagues are looking to expand to a complete entanglement swapping experiment, which would be the first of its kind in frequency encoding. This work is planned as part of ORNL's Quantum-Accelerated Internet Testbed project, recently awarded by DOE.

20.A Look at Quantum Resistant Encryption & Why it's Critical to Future Cybersecurity

by Casey Crane
https://www.thesslstore.com/blog/quantum-resistant-encryption-why-its-critical-to-future-cybersecurity/

Quantum resistant cryptography will be a key part of cybersecurity in the future. Here's what to know about how to protect your data when hackers are armed with quantum computers

Quantum computing is a contentious topic that people tend to either love or hate depending on where they're seated. On one hand, it represents an incredible opportunity in terms of data processing speeds and capabilities. On the other, it's a means through which to destroy the cryptographic algorithms we now rely on to keep sensitive data secure online. This is where something known as quantum resistant encryption comes into play.

But what is quantum resistant encryption? This article explores the history of quantum computing in cryptography, why it's a threat to modern online security, and what organizations can do to prepare to implement quantum safe cryptography within their IT environments.

What Is Quantum Resistant Encryption? Explaining Quantum Safe Cryptography

In a nutshell, quantum resistant encryption refers to a set of algorithms that are anticipated to remain secure once quantum computing moves out of the lab and into the real world. (They will replace the public key cryptography algorithms currently used by billions of people around the world every day.)

By the way, when people use any of the following terms, they're typically talking about the same

thing (in most cases):

- Quantum resistant encryption
- Quantum resistant cryptography (QRC)
- Quantum safe cryptography
- Post-quantum cryptography (PQC)
- Post quantum encryption

All of the public key encryption algorithms we currently rely on today are expected to be broken once researchers succeed in building large enough quantum computer. Once that happens, quantum resistant encryption will need to be used everywhere (both by "normal" [i.e., "classical"] and quantum computers) so that attackers with quantum computers can't break the encryption to steal data.

Why Will Quantum Computers Break Current Encryption Standards?

Quantum computers are fundamentally different from the computers we use today. These devices use specialized hardware components that bring quantum physics into the equation and allows them to perform certain calculations exponentially faster than even the fastest supercomputer we currently have. (We'll speak to that more later in the article.)

Current public key cryptographic algorithms rely on complex mathematics (for example, the RSA encryption algorithm relies on factoring prime numbers while Diffie-Hellman and elliptic curve cryptography, or ECC, rely on the discrete logarithm problem) to securely transmit data. This means that every time you buy an item on Amazon, your browser communicates with Amazon's web server via a mathematically derived secure communication channel based on one of these mathematical approaches.

The problem is that some quantum computers will be able to solve these mathematical problems so quickly that hackers would be able to break modern public key encryption within minutes. (Basically, rendering the encryption public key algorithms provide useless.)

According to the National Security Agency (NSA), quantum resistant cryptography should be "resistant to cryptanalytic attacks from both classical and quantum computers." With this in mind, these algorithms would be something that can be used both before and after quantum computers are put to use in real-world applications. They're designed with quantum computing threats in mind, but they're not limited to being used only after a cryptographically relevant quantum computer (CRQC) is created.

Modern Algorithms vs Post Quantum Encryption Algorithms

Currently, encryption over insecure channels (e.g., the internet) relies on something known as public key cryptography. The idea behind traditional public key algorithms is that two parties (i.e., your website's server and the customer who wants to connect to it) can communicate securely using two separate but related keys: a public key that encrypts data and a private key that decrypts it. They use these keys to exchange secret information that they can use to create a secure, symmetrically encrypted communication channel. (Why symmetric encryption? Because it's faster and less resource-

intensive than public key encryption.)

Unlike modern algorithms, quantum resistant encryption algorithms will replace existing public key specifications with ones that are thought to be quantum resistant. Again, this is because the modern digital signature and key establishment algorithms we rely on in public key encryption now will no longer be secure when CRQCs become a thing.

NIST says that quantum resistant algorithms typically fall in one of three main camps:

- **Code-based cryptography** — These are algorithms that rely on "error-correcting codes."
- **Lattice-based cryptography** — These algorithms involve matrices based on geometric structures.
- **Multivariate public key cryptosystems** — These types of algorithms vary based on the type of problems they're trying to solve.

There is a fourth category that some reference — stateful hashed-based signatures. But according to NIST's PQC FAQs page:

"It is expected that NIST will only approve a stateful hash-based signature standard for use in a limited range of signature applications, such as code signing, where most implementations will be able to securely deal with the requirement to keep state."

What Would Be Considered a Quantum Resistant Encryption Algorithm?

We can't give you a specific answer here because, well, nothing has really been decided yet. The NIST has been engaged in a large-scale cryptographic competition of sorts for the past several years. The competition is an opportunity for mathematicians, researchers, cryptographers, educators and scientists to submit algorithms for consideration as future federal standards.

The standards body announced their selection of seven candidates and eight alternate algorithm candidates from the third round of submissions. However, no final decisions have been made regarding which algorithm(s) will be standardized:

- 4 public key encryption and key-enablement algorithms (Classic McEliece, CRYSTALS-KIBER, NTRU, SABER)
- 3 digital signature algorithms (CRYSTALS-DILITHIUM, FALCON, Rainbow)
- 5 alternate public key encryption and key enablement algorithms
- 3 alternate digital signature algorithms

What Is Quantum Computing?

To better understand quantum resistant encryption and why it's needed, you first need to understand quantum computers and their anticipated impact on cyber security. The idea behind quantum computing is that these devices use quantum mechanics to approach problem solving — the general goal of all modern computers — in a whole new way and at exponentially faster speeds.

According to research from Mavroeidis, Vishi, Zych, and Jøsang at the University of Oslo, Norway, there are two types of quantum computers:

- **Universal quantum computers** — As the categorical name implies, these devices are designed to perform virtually any task

- **Non-universal quantum computers** — These machines are, essentially, designed for specific purposes to handle specific tasks. For some tasks, they aren't anticipated to be much faster than classical computers.

At a basic level, the computers we use today (classical computers) communicate data using specific combinations of 1s and 0s (binary numbers called bits). All modern computers play by these same rules. For example, if I type the word "Howdy!" the computer uses this combination of bits to communicate the precise combination of keys I press: 01001000 01101111 01110111 01100100 01111001 00100001.

A basic illustration that shows the translation of individual characters and symbols of the message into binary.

Quantum computers, on the other hand, operate on a new playing field using a different set of rules. Instead of these traditional bits (1s or 0s), it relies on quantum bits, or qubits for short. In a nutshell, instead of looking at either 1s or 0s, quantum computers view data as existing in multiple states, meaning that it can be both 1s and 0s simultaneously (this is known as a superposition). It also uses two other quantum properties — entanglement and interference — to connect separate data elements and eliminate irrelevant guesses to solve problems more quickly.

Of course, not all qubits are the same. Microsoft recently announced that their Azure Quantum program has unlocked the first step to developing a new type of qubit called a topological qubit. The goal is to resolve the scaling-related issues that other quantum computers face and to eventually help lead to the creation of a quantum computer capable of employing one million or more qubits. (Check out the linked article for more information on Microsoft's demonstration.)

We're not going to get into all of the technical aspects of the other quantum properties we mentioned here, either.

The takeaway we want you to have is that, on one hand, some quantum computers are poised to solve problems beyond what modern supercomputers can do — but faster and more efficiently. They also have the potential for other unimaginable capabilities to do things we haven't even thought of yet. On the other hand, some quantum computers are anticipated to be no better than classical computers for some types of tasks. But trying to predict the future in terms of the full impact of quantum computers in the future is easier said than done.

Why Quantum Computing Is Thought to Pose a Threat to Modern Cyber Security

Our understanding of quantum computing is largely theoretical — so far, quantum computers can only

be used in laboratories due to the machines' massive resource and cooling requirements. Quantum chips have to be kept super cold (at -273 degrees Celsius, or what amounts to nearly absolute zero) to operate, and they can only operate for very short bursts. But the concern that cybersecurity and industry leaders have is that as quantum computers eventually become more mainstream, they'll make existing public key encryption algorithms — namely, RSA (Rivest Shamir Adleman) — essentially useless.

This concern is due to a concept known as Shor's Algorithm. The basic overview of the concern about this algorithm, which was first demonstrated in 1994 by the guy who created it (mathematician Peter Shor), is that a powerful enough quantum computer would be able to crack modern public key algorithms pretty much instantly. How would it do this? By having the ability to calculate the factors of enormous numbers — i.e., the math that operates at the very heart of modern public key encryption — at faster rates than any modern devices could manage.

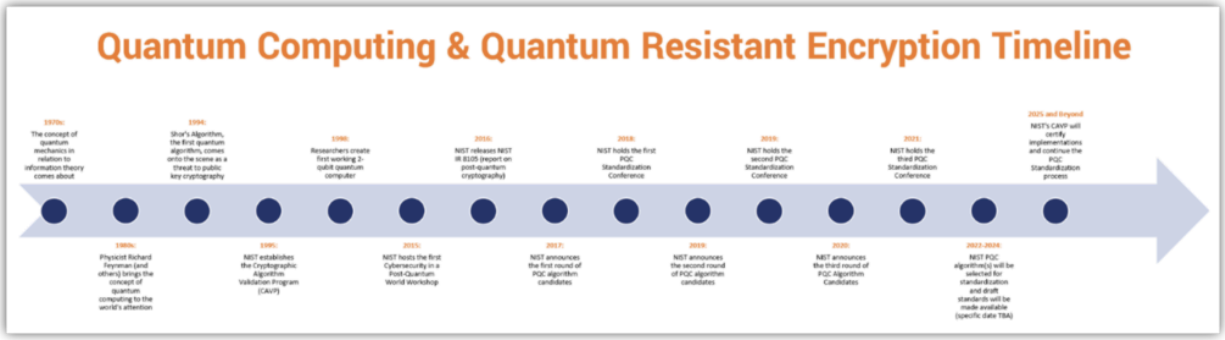
When you try to crack asymmetric encryption (say, RSA) using a classical computer, you're essentially trying to guess the factors of those mega-sized integers. As you can imagine, this will take a really long time using a regular computer. But with quantum properties like superposition, entanglement and interference coming into play, it can reduce the time required to make those guesses (or eliminate the need to guess some of the numbers entirely) to basically nothing. For example, while it would take upwards of millions of years for traditional computers to figure out the prime factors of 2,000+ bit numbers, a quantum computer could complete the same task within minutes.

While this enhanced speed will be great for creating positive solutions to problems — such as coming up with revolutionary new treatments or cures for medical conditions — it also poses a problem if these devices fall into the wrong hands.

A Look at the PQC Timeline

Now, we're not telling you all of this to scare you. The truth is that the threats that quantum computing represents aren't new concepts, nor do they represent threats to your business and customers right now. The concept of quantum computing — and all of its benefits and dangers — has been around for decades and isn't expected to come to fruition yet.

Here's an overview of the history of quantum computing and how the development of quantum resistant cryptography plays a key role in it:



A graphic timeline of quantum computing over the last six decades, including NIST's post-quantum

cryptography-focused initiatives (workshops, conferences and announcements).

Here are links relating to some of the points on the timeline above:

- 1980s: Researchers (including Richard Feynman) helped bring about the study of quantum computation
- 1994: Peter Shor presents his paper "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer"
- 1997: Researchers create the first 2-bit quantum computer
- 2016: NIST Publishes IR 8105 (Report on Post Quantum Cryptography)
- 2019: PQC First Round of Candidates Announcement
- 2020: PQC Sound Round Candidates Announcement
- 2021: PQC Third Round Candidates Announcement

So, how long is all of this expected to take? The answer depends on who you ask and in what context:

- The NIST says it can take 10-20 years "from deciding a cryptosystem is good until we actually get it out there as a disseminated standard in products on the market."
- The NSA says that "new cryptography can take 20 years or more to be fully developed to all National Security Systems."

As you've probably seen, change tends to be relatively slow in the cryptographic world. Let's think about it another way. When TLS 1.2 was developed, TLS versions 1.1 and 1.0 were outmoded, but they're still in use on the web and haven't gone away completely. (We're at 14 years and counting at this point since TLS 1.2 was initially released and we now have TLS 1.3, which came out in 2018!)

As we touched on earlier, NIST is working on finalizing the selection of the final algorithms that will become standardized. Once final PQC algorithms are selected, then the next move will be to publish PQC standards as Federal Information Processing Standards (FIPS) and move on to implementations and deployments. Once this occurs, the Cryptographic Algorithm Validation Program (CAPV) will provide certifications for approved implementations of these approved PQC algorithms.

We bring this all up now because we're drawing closer to a future when quantum computers are anticipated to become mainstream. It won't happen today, tomorrow, or likely even five years from now. But when it does, organizations will need to be able to support and use the quantum resistant encryption algorithms necessary to help keep data secure in this super-powered computer processing world to come. And things are changing now to prepare for that inevitable future.

A Look at the Changing Landscape Surrounding Quantum Resistant Encryption

On Jan. 19, 2022, the White House released a memorandum specifying that agencies have 180 days to "identify any instances of encryption not in compliance with NSA-approved Quantum-Resistant Algorithms or CNSA [...]" and must report the following to the National Manager:

- What systems are noncompliant (including those with exceptions or waivers)
- A timeline for how these systems will transition to compliant encryption, and

- Any reasons why any systems should be exempt from compliance

What does all of this mean at the level of your organization or company? In reality, not much right now for everyday businesses. But let's be realistic here — it's virtually impossible to be compliant with rules that haven't yet been implemented. It's kind of like playing a new sport — say, soccer — when you don't yet know the rules or how to play it. Sure, you can go through the motions and move the ball down the field. But if you don't know how you're supposed to do it or which goal to aim for specifically, no telling if you're doing it right or if you're moving in the right direction.

The NIST was anticipating the release of its PQC Round 3 Report by the end of March or early April 2022. (There's also been talk about announcing a fourth round of study as well.) Now, in all fairness, we've just started the month of April a week ago. But considering that agencies are expected to be compliant with quantum-resistant algorithms by basically July 2022, and the algorithms themselves haven't officially been decided upon… well, that sure makes things a lot more difficult for organizations that have to be compliant.

However, once NIST decides which algorithm(s) will become the standard, then it's up to businesses and organizations to ensure that they're not using or relying upon any algorithms that may have been deprecated. The standards body is expected to have draft PQC standards available for public comment before the end of 2023 and aims to have a finalized standard ready the following year.

Although the Sky Isn't Falling… Yet — Now's the Time to Prepare

You'll find that many experts typically sit in one of two camps when it comes to the topic of quantum computing and quantum resistant cryptography. On one end of the spectrum, the first camp — aptly named "Panicville" — essentially operates under the assumption that the end of near! Cybersecurity as we know it is about to come crashing down around us at any moment! BEWARE!

The second camp, which we've named "Chillville", tends to take very different approach. The perspective here is typically that quantum computing is still a long way off, that it's too impractical for real-world applications, or that it's something we likely won't have to deal with for years to come, so there's no point in worrying about it now.

Needless to say, neither of these approaches is particularly healthy or beneficial to the security of your organization and its data. Thankfully, though, other experts tend to fall somewhere in the middle — let's call it "Preparationville." The purveying mindset of experts who sit within this space between the two main camps is that:

- Quantum computing poses a serious threat to modern public key-based security (recognize the threat),
- It's still going to take a while for this threat to come to life in the real world (stay calm, don't panic), and
- Organizations should be taking steps now to start getting ready for when it does (make plans and start implementing them now).

Here at Hashed Out, we definitely fall more in the middle of the spectrum; we're not panicking about

the changes to come but are strongly encouraging customers to start preparing now to the best of their abilities. The NSA shares on its Post-Quantum Cybersecurity Resources site that while it doesn't know "when or even if" a system capable of cracking public key encryption will make its debut. However, it does make it clear that preparing for an "eventual transition" to post-quantum cryptographic standards is a must for data security in the future.

Better to be safe than sorry, right?

It's Time to Start Preparing for the Inevitable By Planning & Investing In Resources Now

Great. So, you're being told to prepare, but it's hard to prepare for something when you don't really know what tools you'll have at your disposal to work with. It's like trying to prepare for a disaster as a homeowner — you might not know when something bad will happen, but you're going to take steps to mitigate potential impacts as much as possible.

The same concept here applies with preparing for quantum cryptography. While you may not know which algorithms specifically will be standardized, or specifically when quantum resistant cryptography will need to be implemented, you know it's likely going to happen and that you should take steps now to prepare for it.

Develop Your Organization's PQC Plan (Be Sure to Include Specific Milestone Dates)

We get it — there's definitely a strong case of "you don't know what you don't know" going on here. However, you can take steps to stay ahead of the curve as much as possible by taking the time to research and plan your strategy now. Part of this planning should include:

- Prioritizing which systems to transition first, starting with the most sensitive and at-risk resources, as well as those that are integral in terms of your organization's goals and needs
- Designating who is responsible for different aspects of the implementation

Audit Your IT Environment and Cryptographic Systems

We can't overstate the importance of this task as it's something you should already be doing anyhow. Auditing your organization's cryptographic systems, IT infrastructure and applications is crucial for a multitude of reasons. Furthermore, it can aid you as well with the development of your PQC planning and deciding what gets upgraded and when.

Begin Upgrading Your IT Infrastructure and Related Resources

If your organization is running on older servers and other related infrastructure, you're likely to need to upgrade before quantum cryptography makes its debut. Something to consider includes having servers with redundant distributed databases that use PQC digital signature algorithms that are connected via quantum key distributed (QKD) connections. (QKD is a concept that's been around since the 80s and involves using quantum mechanics to distribute keys between communicating parties in tradi-

tional symmetric algorithm-protected connections.) The idea here is that this may help to protect against quantum attacks and aid in recovery from successful attacks.

What about hardware security modules? Is your organization using one in-house? Is it relying on a third party system? Ensure that whatever HSM you're using has a roadmap to support quantum safe encryption.

We understand your hesitation and dread — updating your existing infrastructure is a massive undertaking. It involves major investments in money, time, and personnel-related resources. But this is why it's crucial to start planning for and begin implementing these upgrades now. If you roll out the upgrade to your systems over time, it means you won't have to blow all of your capital budget in a single year or two, or risk rushing implementation (which can lead to mistakes) because you decided to wait until crap hits the fan.

Essentially, you're carefully preparing for the impending storm ahead of time (as much as you can). This way, your organization will be less likely to get caught in the downpour others will get swept away in.

Upgrade Your Existing Cryptographic Security Measures

The NSA also offers the Commercial National Security Algorithm Suite (CNSA Suite), which is a set of algorithms that the Committee on National Security Systems Policy 15 (CNSSP-15) has identified for protecting classified information (listed in alphabetical order):

Algorithm	Key Size / Curve Size	Usage
AES-256	256 bits	Confidentiality (encryption)
Diffie-Helman (DH)	3072 bits or higher	Key establishment
Elliptic Curve Diffie-Hellman (ECDH)	384 bits	Key establishment
ECDSA	384 bits	Digital signatures
Rivest Shamir Adleman (RSA)	3072 bits or higher	Key establishment and digital signatures
SHA-384	384 bits	Integrity protection (hashing)

Broken cryptosystems are the ugly companion of all the advancements that quantum computing has to offer. This is why major certificate authorities like DigiCert and Sectigo are working now to help prepare for a PQC world on their ends by creating PQC certificate authorities (CAs) and certificates.

DigiCert, which plays a key role in multiple PQC projects, offers a PQC Toolkit to Secure Site Pro customers. This toolkit offers hybrid RSA/PQC certificates, which pair PQC algorithms with classical ones. The goal here is for these certificates to work on both legacy systems (to offer backwards compatibility) and quantum systems once quantum computers finally roll out.

DigiCert estimates that it would take a traditional computer "a few quadrillion years" to break modern 2048-bit encryption. But considering that we don't know exactly when quantum devices are going to come charging onto the scene, it's a good idea to start preparing now for when it does happen. This is why the CA also has created a resource that breaks down the Post Quantum Cryptography Maturity Model. You can use this to figure out how well prepared your organization is (or isn't) for what's the come.

Sectigo's Senior Vice President of Product Management Lindsay Kent spoke during one of the company's Identity-First Summit 2022 presentations on certificate lifecycle management. Kent said that the certificate authority expects to have quantum safe security in place by 2026. The plan includes providing customers with a "Quantum Safe Toolkit" as well that aims to help companies:

- Evaluate quantum-safe interoperability with applications
- Create a quantum safe certificate authority to issue certificates using quantum-safe certificate chains
- Issue certificates that can be installed into applications

The goal here for both CAs is to help companies use these certificates to facilitate quantum safe application-based authentication (instead of network-based authentication) and secure communications via TLS sessions. It's also to ensure that organizations can have certificates in place that support both PQC algorithms and the traditional algorithms that we have in place now.

Wait, doesn't offering backwards compatibility mean that users on classical devices will still be connecting via protocols relying on insecure algorithms once quantum computers become mainstream? Yes. But if you want to continue providing services to customers using legacy systems, that's going to continue until they eventually make the change.

Review and Update Your Security Procedures and Protocol Resource Documents

An important part of the planning we talked about earlier is taking the time to review and make changes to your organization's existing internal security procedures and related documentation. Some of the things you'll want to consider is what quantum resistant secure access controls and authentication measures you'll need to implement. As you've probably guessed, your existing controls won't cut it in a PQC world, so everything will need to be updated to be quantum resistant once NIST publishes its standards.

Final Thoughts on Preparing Your Organization to Support Quantum Resistant Encryption

As we talked about earlier, the widespread use of quantum computing — and, therefore, the deployment of quantum resistant cryptography — is still on the horizon but is likely at least a good decade or so away. But that's why now is the time to prepare for PQC to help your business stay ahead of the curve. You don't want to be one of the organizations caught unprepared when quantum computers make their mainstream debut.

21.Quantinuum Announces Quantum Volume 4096 Achievement

by Kortny Ralston-Duce
https://www.quantinuum.com/pressrelease/quantinuum-announces-quantum-volume-4096-achievement

Quantinuum has reached another milestone in its quest to build the highest performing quantum computer in the world.

This week, the System Model H1-2 doubled its performance to become the first commercial quantum computer to pass Quantum Volume 4096, a benchmark introduced by IBM in 2019 to measure the overall capability and performance of quantum computers.

It marks the sixth time in two years that Quantinuum's H-Series hardware, Powered by Honeywell, has set an industry record for measured quantum volume.

The achievement also fulfills a March 2020 promise made by Honeywell Quantum Solutions, which combined with Cambridge Quantum in late 2021 to form Quantinuum, to increase the performance of its trapped ion technologies by an order of magnitude each year for the next five years.

"This is the second consecutive year we've delivered on that promise and our commitment to developing the highest performing quantum hardware available," said Tony Uttley, president and chief operating officer at Quantinuum.

Continuous upgrades

This week marks the second time in four months that the System Model H1-2, which came online late last year, has achieved a quantum volume milestone. It set a record in December 2021 when it passed Quantum Volume 2048.

Uttley attributed the doubling of performance to the consistent upgrades that are made.

Quantinuum currently operates two commercial quantum computers, the H1-1 and H1-2, which run projects for customers and then are taken offline for upgrades.

"This approach provides the opportunity for us to continuously add new updates and features to our systems, which enables us to improve performance," he said. "We learn a lot about our machines by running projects and can make small upgrades or tweaks that keep our fidelities high."

The data

The average single-qubit gate fidelity for this milestone was 99.994(3)%, the average two-qubit gate

fidelity was 99.81(3)% with fully-connected qubits, and measurement fidelity was 99.72(5)%. The Quantinuum team ran 200 circuits with 100 shots each, using standard QV optimization techniques to yield an average of 152.97 two-qubit gates per circuit.

The System Model H1-2 successfully passed the quantum volume 4096 benchmark, outputting heavy outcomes 69.04% of the time, which is above the 2/3 threshold with greater than 99.99% confidence.

The team used a new method developed by Quantinuum researchers, Dr. Charlie Baldwin and Dr. Karl Mayer, to calculate the confidence interval.

What's next?

Uttley said the next step is to increase the number of qubits on both Quantinuum machines and to continue to improve gate fidelities.

"The System Model H1-2 used all 12 of its fully connected qubits to pass Quantum Volume 4096," he said. "We have reached the limit of what we can do with 12 qubits. To continue to improve performance, we need to add qubits. So keep watching what happens soon."

22.The Quantum Insider Celebrates World Quantum Day: Quantum Computing Timeline

by James Dargan

https://thequantuminsider.com/2022/04/14/the-quantum-insider-celebrates-world-quantum-day-quantum-computing-timeline/?utm_source=newsletter&utm_medium=email&utm_term=2022-04-21&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Horizon+Expands+With+%2412+Million+Series+A+National+Quantum+Day+--+And+More+Quantum+News

As today (April 14) is World Quantum Day, a time when everything Quantum is celebrated, The Quantum Insider thought it a good idea to highlight some of the major milestones in the development of the industry. Starting way back in the mid-1970s, we take a brief look at some of the seminal moments in Quantum Computing.

Since 2019, the market and interest in QC has rapidly accelerated – we will soon be able to do a whole detailed timeline of innovations over the last few years.

Happy World Quantum Day!

Year	Major Milestones Developed
1968	Stephen Wiesner invents conjugate coding
1976	Polish mathematical physicist Roman Stanislaw Ingarden publishes a seminal paper entitled "Quantum Information Theory" in Reports of Mathematical Physics Vol. 10, 43-72, 1976. (It was submitted in 1975.) It is one of the first attempts at creating a quantum information theory, showing the Shannon information theory cannot directly be generalised to the quantum case, but rather that it is possible to construct a quantum information theory which is a generalisation of Shannon's theory, within the formalism of a generalised quantum mechanics of open systems and a generalised concept of observables (the so-called semi-observables)
1980	Paul Benioff describes the first quantum mechanical model of a computer. In this work, he showed that a computer could operate under the laws of quantum mechanics by describing a Schrödinger equation description of Turing machines, laying a foundation for further work in quantum computing. This paper was submitted in June 1979 and published in April 1980. Yuri Manin briefly motivates the idea of quantum computing
1981	At the First Conference on the Physics of Computation, held at MIT in May, Paul Benioff and Richard Feynman give talk on quantum computing. Benioff's built on his earlier 1980 work showing that a computer can operate under laws of quantum mechanics. The talk was titled "Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: application to Turing Machines." In Feynman's talk, he observed that it appeared to be impossible to efficiently simulate an evolution of a quantum system on a classical computer, and he proposed a basic model for a quantum computer
1985	David Deutsch, at the University of Oxford, describes the first universal quantum computer. Just as a universal Turing machine can simulate any other Turing machine efficiently (Church-Turing thesis), so the universal quantum computer is able to simulate any other quantum computer with at most a polynomial slowdown.
1992	David Deutsch and Richard Jozsa propose a computational problem that can be solved efficiently with the determinist Deutsch-Jozsa algorithm that they were capable for performing some well-defined computational task more efficiently than any classical computer.
1994	Peter Shor at AT&T's Bell Labs in New Jersey, discovers an important algorithm. It allows a quantum computer to factor large integers quickly. It solves both the factoring problem and discrete log problem. Shor's algorithm can theoretically break many of the cyrptosystems in use today. Its invention sparked a tremendous interest in quantum computers.
1996	Lov Grover, at Bell Labs, invents the quantum database search algorithm. The quadratic speedup is not as dramatic as the speedup for factoring, discrete logs, or physics simulations. However, the algorithm can be applied to a much wider variety of problems. Any problem that has to be solved by random, brute-force search, can take advantage of this quadratic speedup (in the number of search queries)

Year	Major Milestones Developed
1998	First experimental demonstration of a quantum algorithm. A working 2-qubit NMR quantum computer is used to solve Deutsch's problem by Jonathan A. Jones and Michele Mosca at Oxford University and shortly after by Isaac L. Chuang at IBM's Almaden Research Center and Mark Kubinec and the University of California, Berkeley together with coworkers at Stanford University and MIT.
1999	D-Wave Systems Inc. the first commercial quantum computing company, founded in Burnaby, Canada.
2004	First working pure state NMR quantum computer (based on parahydrogen) demostqrsted at Oxford University and University of York
2008	Quantum bit stored
2015	D-Wave Systems Inc.announced on June 22 that it had broken the 1000 qubit barrier
2019	IBM Q Syystem One (2019), the first circuit-based commercial quantum computer IBM unveils its first commercial quantum computer, the IBM Q System One, designed by UK-baaed Map Project Office and Universal Design Studio and Manufactured by Goppion A paper by Google's quantum computer research team was briefly available in late 2019, claiming the project has reached quantum supremacy

23.ARTEMIS: A New European Research Project to Develop Neural Networks for Quantum Error Correction

by Karine
https://thequantumhubs.com/artemis-a-new-european-research-project-to-develop-neural-networks-for-quantum-error-correction/

Quantum Machines, Alice&Bob and European quantum computing research groups led by Prof. Benjamin Huard from the Ecole Normale Supérieure de Lyon and Prof. Florian Marquardt of the Max Planck Institute for the Science of Light, has announced the launch of Project ARTEMIS.

The 3-year project will work to establish and commercialize a radically new approach to quantum control based on Neural Networks.

Project ARTEMIS will work to overcome two of the main challenges in Quantum Computing: Quantum Error Correction (QEC) and optimal control. To accomplish this, the research will focus on the devel-

opment of a quantum controller that incorporates real-time neural networks capable of generating controls. This is set to resolve one of the main bottlenecks towards scaling up error correction and optimal control methods.

The expected outcomes of the project are:

- The deployment of a universal quantum controller with a user-friendly interface and accompanying open-source code libraries for the implementation of the new approach on a variety of quantum processors and devices.

- The public availability of a cloud-based quantum processor with a unique user interface, allowing for the programming and execution of a rich variety of real-time neural networks. This will allow researchers to explore the new approach toward practical quantum computing and quantum sensing, even if they do not have direct access to quantum hardware.

The project will utilize the combined expertise of the participating companies and institutions in the fields of microwave engineering, machine learning, control theory, experimental quantum physics, commercial product design, and realization. Industrial level quantum computers will be used to realize the full potential of the project.

24.Building The World's First Blockchain Geospatial Network Backed With Cryptography

by Anusuya Datta
https://www.geospatialworld.net/prime/building-the-worlds-first-blockchain-geospatial-network-backed-with-cryptography/

The interest in cryptocurrencies has brought a lot of focus on blockchain technologies. However, one major area where blockchain can be used effectively along with geospatial technologies is the Internet of Things. As technologies and data collection and processing get more complicated, the questions are what is the data, how is it validated, how is the proof of location established, how are things and humans protected from illegal access and processes?

XYO Network is the world's first blockchain geospatial network backed with cryptography that anonymously collects and validates data with a geographic component. XYO calls itself the Reality Oracle, a technology protocol designed to improve the validity, certainty, and value of data. It is seeking to build a data marketplace that gives users a gold-standard for any apps, websites, and blockchain technologies that rely on trusted data.

We caught up with **Markus Levin, the Co-Founder XYO Network**, for an interview. Levin also serves

as **Head of Operations for XYO's parent company XY Labs**. XY Labs provides a connection between the real and digital worlds through blockchain, IoT, and data-focused products, which can be leveraged to make human lives easier. For example, the COIN App empowers its over 3 million users to be rewarded for validating geospatial location and other data.

Levin has more than 15 years' experience in building, managing, and growing companies in hyper-growth industries around the globe. He mined his first bitcoin in 2013 and has been captivated by blockchain technologies ever since.

In this interview Levin talks about his vision for XYO, the link between hyper location and blockchain, and how it is all addressing real-world challenges.

Tell us about some notable XYO use cases within industries such as insurance, supply chain, banking, infrastructure, public safety, and more?

XYO's decentralized network of devices anonymously collects and validates data associated with geography, temperature, humidity, and even speed, among other components. While the nature of geospatial data has been historically complex and cumbersome to leverage, XYO's advancements in the area, along with industry collaborations, are allowing commercial enterprises to tap into and harness this information like never before.

Geospatial data is often used to develop consistent, up-to-date, and accurate representations of the physical and digital world, i.e., the metaverse and other virtual spaces.

Acting as a Reality Oracle, XYO harnesses the power of data to address real-world challenges in various scenarios — from directing disaster response to more accurately assessing underwriting risk, analyzing behavioral patterns, and even addressing supply chain issues.

Notable use cases include:

- Addressing supply chain issues by identifying disruptions and bottlenecks in real-time
- Providing insights to plan, design, build, and maintain infrastructure efficiently (i.e., analyzing traffic patterns).
- Bolstering public safety by monitoring dangers such as weather incidents and pandemic outbreaks in real-time.

XYO utilizes proprietary data and all the data provided to the network is processed as real-time information, analyzed, archived, and then acted upon accordingly.

What was your vision of XYO when you launched it and how it is evolving?

Our mission is to create software and devices that focus on location and geospatial data to build a global data network that connects the physical world to the digital world. With our community, we're creating a system of location oracles that will improve current and future location data systems through data that can't be changed.

XYO calls itself the world's first Reality Oracle, which empowers people to participate in the global data economy through the validation of anonymous and secure geospatial data.

XYO has created a reliable Data Ocean, meaning it collects data from various sources and pools it together for verification and analysis. Just as rivers flow towards an ocean, "rivers" of data from the nodes in the XYO Network all run towards the larger XYO Data Ocean, providing an aggregated place for data. After the data is collected and aggregated, the cryptographic protocol can help validate and improve the trust for that collected data.

Data is the currency of the future. Ensuring people's security and agency in the data economy is critical to the quality of life. XYO educates and empowers the people who will be most affected by the data revolution — those who create the data. We believe most people don't fully understand the power and value of the data they generate every single day. XYO educates users about that power by encouraging them to harness it.

Tell us more about the XYO Token and how it works.

The XYO Token ($XYO) is an Ethereum-based ERC-20 utility token used to calculate smart contract agreements on XYO Network. With over four million nodes for the XYO Network, XYO Token is being rapidly adopted. An analysis of 500 users showed XYO-USD portfolio growth of over $14 million as of August 2021.

In January, $XYO was listed on Huboi, one of the leading and most secure digital asset exchanges in the world with over 10 million users.

The coin powers a decentralized network of devices that anonymously collects and validates geospatial data, and also prevents devices from spoofing their location. On the XYO World platform, XYO tokens can be traded for and staked against unique ERC-721 tokens representing real-world locations.

XYO recently announced the launch of its newest network version, XYO 2.0. How will it empower developers?

XYO 2.0 makes the data collected by our users easy for partners to access and utilize. By building functionality with JSON and accessibility through APIs, the data is secure and virtually tamperproof given XYO 2.0's blockchain and cryptographic technology.

XYO provides SDKs ready for immediate implementation, so developers can plug right into XYO and produce cutting-edge solutions for their projects.

The technology protocol that we have designed is singular and can be implemented in any project, in any place, in many different coding languages. The data source doesn't matter since XYO uses a unique cryptographic protocol to ensure data verification and trust.

XYO has really been on the move. Could you tell us a bit more about your re-

cent activities?

February was an impressive month for XYO. We announced a strategic co-investment with Outliers Fund, a collective of joint research initiatives and venture funds with top blockchain ecosystems, and Analog, the first company that is a true Layer-0 protocol powered by blockchain technology—all of these developments, are to accelerate projects built around the XYO Network.

We're also excited to announce our partnership with HERE Technologies, a location solutions company, last year. As leaders in location technology, the collaboration represents an opportunity to expand the availability of secure, verified geospatial data and to bridge real-world location data with blockchain-based smart contracts. With XYO's ability to capture, index, and store location data and HERE Technologies' powerful geospatial mapping capabilities, the partnership stands to unlock a treasure trove of advancements in location data and technology.

XYO has also developed and strengthened pivotal partnerships with key players in the web3 community, including Chainlink, Microsoft, Dispatch Labs, and Harmony. As we continue to focus on maximizing education surrounding our open source code protocol, we look to partner with more industry leaders in the future.

And, of course, a wide array of exchanges have recognized the value of the XYO Network and the XYO token in recent months. The accomplishment represented by these listings results from the forward-thinking nature of those exchanges and our diligent team.

Where is XYO headed next, and how has the company pivoted in the wake of innovations in technology, specifically data location?

As we look to the remainder of 2022 and beyond, XYO is excited about new projects and partnerships in the pipeline that will continue to drive blockchain technology forward. And as this technology continues to evolve, we're aiming to have a say in how the global, cross-platform metaverse and other virtual spaces take shape—we aim to provide tested solutions to accelerate the growth we all know is ahead.

Here's an example: $XYO is now more widely available, with more exchanges being added regularly. By combining the XYO Protocol 2.0 changes, COIN data producers and purchasers, and XYO Token Payment Channels, we are forging a revolutionary data marketplace that uses XYO tokens as the low-cost payment method for data exchanges without relying on the emergence of a cost-effective decentralized smart contract system.

25.Why Is IBM Selling Post-Quantum Crypto When It's Still A Pre-Quantum Company?

by Rupert Goodwins
https://www.theregister.com/2022/04/11/opinion_column_ibm/

IBM's most exciting mainframe yet, the z16, is finally here. Just three years after the z15, at this rate IBM has until 2212 to buy the z80 trademark from Zilog.

It's good for hybrid cloud, apparently, but the two main advances are real-time AI fraud detection, and "industry-first" quantum-safe cryptography, the stuff that even pesky quantum computers can't crack.

Hold on a qubit. IBM is also pouring billions into exactly those quantum computers, also majoring on real-time fraud detection and cryptography, which means it's squaring off against itself. That might concern investors or customers making strategic decisions, but calm yourselves. Quantum computing doesn't do anything useful yet, nobody can give you a firm date when it will, and it's not as if IBM spaffing billions on a moonshot project means you'll ever get to the moon. Wait and see. It might be a while.

You only have to wait until the end of May to buy a z16, take it home, plug it in and start using it. (Just kidding. It's a mainframe. You can't do any of those things, especially not just buy one. Have you seen the forms?

Hey crypto... it's the future

As an El Reg reader, you probably won't be swayed by the real-time AI fraud detection. The quantum-safe cryptography? That's more intriguing.

Also known as post-quantum cryptography or PQC, it's something you need to know about. IBM's claim that this is an industry first is arguable – practical ways to use PQC have been around for a few years now.

The need for PQC is simple. Everyday cryptography relies on keys built from prime numbers that can't be reversed by brute force using conventional computers. The mathematics is clear. But the math also says that QC can decompose numbers to their primes quickly enough to be useful. Maybe not today, maybe not tomorrow, but soon. When it does, the security that secures the entire Internet won't be safe. We need different math, and PQC is just that. The favorite flavor, and the one IBM is using, is called lattice-based cryptography or LBC and it involves having an enormous multidimensional haystack of points in which you hide your digital needles.

There is no quantum magnet to yank those needles out; you need a mathematical map (the actual math is a little more involved.)

This stuff works. So why aren't we using it yet, and why does IBM think we should?

The first answer is simple: we should be using it. Even if it's years before QC breaks today's codes,

there are plenty of people snooping on and storing transactions right now in preparation for that future. We're not using it for three reasons: there are no standards, there are no standards, and there are no standards. The US National Institute of Standards and Technology is on its third round of evaluation for PQC and is expected to pronounce the standard between 2022 and 2024.

The winning standards for key and signature generation will have to be practical and proven secure, and these are hard targets. It's no good having proven secure systems that take too long, too much power or too much overhead to implement in mobile devices. And while there are candidates that look as good as, or even better than, the current non-PQC options, it's not certain they're safe. But we're almost there: LBC has been known since the 1990s, a very great deal of work has been done on efficiency, use of accelerators and software/hardware co-design. It will be here, and it will be before QC gets its act together.

That's how. But why?

That's the easy bit. It's harder to know why IBM has chosen now to put it into its z16. If the mainframe is Alice, who's Bob? Cryptography that lives in only one place is only good for protecting data at rest, and the real need for PQC is data in flight.

If your encrypted data at rest is compromised, how safe are your keys? Data in flight doesn't have that issue. It could be that IBM is trying the traditional trick of putting an implementation of a non-standardised technology into the field in the hope of forcing the hand of the standards makers, but if that worked with mainframes we'd all be speaking EBCDIC.

So if it doesn't do much for you or just about anyone right now, why is it there? CFAAST - Cryptographic Fear As A Sales Technique. You've got to feel a little sorry for Big Blue: it puts in a very great deal of engineering work into maintaining its position as world leader of mainframes, but it's only competing in that category against itself.

What high performance system these days isn't a huge sea of cores, superfast interconnects, with lashings of screamingly swift memory and fat fast networking to fat fast storage?

IBM has to keep its z/OS customers on board and sell them new kit, even if it is hard to distinguish between carrots and sticks. Yes, oh mighty CEO, our hybrid cloud strategy is now post-quantum secure. You don't want it to be vulnerable to scary quantum computing, do you?

Thus, dear reader, while you can and should be boning up on lattice PQC, I can confidently advise against buying a z16 for the job. Even if it is first. I know, I'm sad too.

26.Why Education Must Take A Quantum Leap

by Alessandro Curioni

https://www.weforum.org/agenda/2022/04/why-education-must-take-a-quantum-leap/

- Quantum computing could have benefits across industries including pharmaceuticals, renewable energy development, finance and manufacturing.
- To fully embrace this technology, however, we need to focus on quantum education and workforce development.
- While some programmes are being rolled out to students and a handful of workforces, more effort is needed to achieve the "quantum advantage".

The 13-year-old daughter of a friend visiting my workplace — the IBM Research lab in Zurich — seemed puzzled. She knew I worked in a research lab and I that work with computers, but the computers she knows don't typically resemble the chandelier-like structure that hung from the ceiling in front of us.

Yet, it is a computer – a quantum computer. And while someone in their early teens right now can be excused for not knowing what a quantum computer is, I would very much like that to change. Quantum computing technology is rapidly maturing and we are on the brink of a technological revolution. Quantum computers work with qubits instead of the much more familiar binary digits, or bits. And while the bits in our current electronics can only have the value of either a 0 or a 1, a qubit can be both at once.

Thanks to this property, among others, quantum computers can perform faster and more precise computations than classical computers. This means they should be particularly well-suited to tasks relying on probabilities and optimization, such as creating a new complex molecule to develop a material with specific properties. There can be a myriad of different arrangements of atoms to form a molecule, and it's incredibly difficult to find the correct one. A quantum computer can quickly sift through all the possibilities to zero in on the most likely candidates.

Accelerating towards the future

The ability to create remarkably fast and accurate molecular simulations makes quantum computers a crucial next-gen tool to accelerate the discovery of new materials - anything from new drugs to solar panels to polymers. In fact, within a few years, these machines should be able to achieve the so-called "quantum advantage", that is, become better than traditional computers at a specific, practical task.

But the question is, once they reach this important threshold, will the world be ready for these machines? Will companies know how a quantum computer could help them? Will university graduates in computer science be able to create a quantum algorithm? And will the necessary infrastructure exist to support hundreds, or even thousands, of these new machines?

If we were to reach a quantum advantage a few years from now, the answer to all those questions would be "no". We are still only at the dawn of our quantum journey. By the time the entire world starts relying on these machines, people won't have to know quantum programming at all. They will

simply choose the right algorithm from a quantum app library, and it will work its quantum magic in the background.

But that's the future. To get there, we need to make the world quantum-ready today by focusing on education and workforce development.

High school quantum and beyond

Kids today should learn about quantum computers as part of their high school education. Before they choose their career paths, young people should learn what this emerging technology will be able to do across industries including material discovery, drug development, finance, space exploration and even manufacturing of the next smartphone.

Beyond high school, quantum computing education should be much more diverse than it is today. To ensure that we have trained enough talent to create new quantum algorithms and to continue to improve the software and hardware, we need to offer quantum computing courses to a much wider range of undergraduates and to those pursuing apprenticeships and other shorter degrees and certificates. We also need to encourage businesses and organisations today to start getting more employees quantum-ready.

There are already early efforts to both educate students and the existing workforce, but there should be more. Globally, not many universities offer quantum programming courses, for example. This education gap could seriously impact the development of a quantum-ready workforce.

Getting an education

The US government has launched an initiative to get high school pupils interested in quantum information science and quantum computing. Dubbed the National Q-12 Education Partnership, the effort unites 15 quantum-driving leaders in industry and academia. The initiative is supported by the White House Office of Science and Technology Policy and National Science Foundation (NSF). The latter has already pledged nearly $1 million for various quantum information science (QIS) education efforts, including the Q2Work programme to get QIS resources into classrooms.

Although there are only a small number of physical quantum computers in the world — including IBM systems in Tokyo and Germany, and soon in Canada and at the Cleveland Clinic in the US — they are all accessible through the cloud. This means anyone from academia or industry, anywhere in the world can access a quantum computer to learn the basics of quantum programming.

At IBM, for instance, there are several quantum-focused education programmes that include access to quantum computers, teaching support, summer schools and hackathons. This includes Qiskit, Qubit by Qubit's Introduction to Quantum Computing in partnership with The Coding School, and the Quantum Educators programme, which gives school teachers and students access to IBM quantum systems through the cloud.

Such efforts are important. Schools and universities worldwide must tackle the quantum education gap

together, setting the next generation of talent on a quantum course from their teenage years.

Building a quantum-ready workforce

When it comes to educating adults, only a handful of companies are currently investing in developing an understanding of quantum technologies. Considering that quantum computers can give businesses an edge, many more should follow suit — be it a pharma giant looking for new drugs or a renewable energy company trying to create more efficient materials for solar panels.

There are many possibilities where quantum computers should be able to help, especially when it comes to finding the best option among a myriad of possibilities — think billions upon billions of configurations for a new molecule.

This is the future, but today's research should get us there remarkably soon. For the world to truly embrace the full potential of quantum computing, we need to focus on quantum education and workforce development. And we need to do it now.

27.Quantum Computing Ecosystem Expands in All Directions

by Veronica Combs
https://www.techrepublic.com/article/quantum-computing-ecosystem-expands-in-all-directions/amp/

It's hard to keep up with all the news coming out of the quantum computing industry these days. The quantum ecosystem is growing in all directions from academic to corporate boardrooms and producing new hardware, software and partnerships.

Denis Mandich, CTO of quantum entropy startup Qrypt, said that the race to make qubits at scale is a winner-take-all competition.

"If you make that scalable quantum computer, your advantage is so great that you'll leave everyone else in the dust," he said. "That's why so much money is pouring into this sector and why companies are hiring at an unbelievable pace."

Qrypt is a member of the Quantum Consortium that tracks open positions among member organizations including corporations, academic institutions, national labs and government agencies. There are more than 600 listings in the QED-C directory as of early April.

"It's a knife fight to get people at this point," he said.

Mandich said every country has outspent the U.S. when it comes to quantum investments because leaders recognize that this is a national race as well.

"Whoever is there first has immediate business interest because people will pay for this tomorrow if it scales," he said.

This roundup of quantum news ranging from advancements in hardware, benchmarking work or strategic investments shows why there are so many jobs and why it's a challenge to fill them.

Accenture Ventures invests in quantum chemistry

The Good Chemistry Company got a vote of confidence via a strategic investment from Accenture Ventures, the consulting company's corporate venture capital arm. The company's QEMIST Cloud is an integrated platform designed for developers. Computational chemistry developers can use the platform to build chemical simulation applications and workflows with emerging algorithms in quantum chemistry, machine learning and quantum computing.

Carl Dukatz, Accenture's global quantum computing lead, said in a press release that a new class of scalable cloud-based technology is emerging to support the next generation of chemistry, material science and structural design. Accenture Ventures did not disclose the terms of the investment.

Pasqal partners with Siemens and Microsoft

Siemens Digital Industries Software is funding a research project with Pasqal to advance quantum computational multi-physics simulation. The company will use its proprietary quantum methods to solve complex nonlinear differential equations and enhance Siemens' product design and testing software. Pasqal specializes in neutral atom-based quantum computing.

Georges-Olivier Reymond, CEO and founder of Pasqal, said the work will focus on creating more accurate digital twins for automotive, electronics, energy and aerospace customers. Pasqal's quantum technology controls atoms with an equal number of electrons and protons with optical "tweezers" and laser light to engineer full-stack processors with high scalability and long coherence times, according to the company. The company's software agnostic processing units operate at room temperature with lower energy.

In March, the French company announced a partnership with Microsoft to offer access to its technology via Azure Quantum. Dr. Krysta Svore, a distinguished engineer and VP of quantum software at Microsoft, said Pasqal's services will provide Azure Quantum users with new computational possibilities. The Pasqal system will be available later this year.

Zapata and IonQ win DARPA award

Zapata and IonQ announced at the end of March a Defense Advanced Research Projects Agency multi-million dollar award for quantum benchmarking. The funds will support the creation of software tools to make hardware-specific resource estimates for quantum computers. The collaboration includes teams from:

- Aalto University, Finland

- IonQ
- University of Technology Sydney
- University of Texas at Dallas
- Zapata Computing

Yudong Cao, CTO and founder of Zapata Computing, said the program will focus on hardware-specific resource estimation.

"The key priority is building and integrating software tools across a broad range of the quantum stack from abstract program description, compiler toolchains, error correction and mitigation, to low-level physical control of quantum hardware systems," Cao said. "For Zapata specifically, this program will also be an opportunity to test and develop our Orquestra platform for large-scale numerical experiments needed for creating the quantum benchmarks."

The research team started work in March and expects the project to last three years.

NVIDIA announces quantum progress

At the GTC conference in March, NVIDIA shared an update on its quantum work. The company's cuQuantum is now in general release, while its cuQuantum DGX Appliance is in beta. CEO Jensen Huang announced a new quantum compiler: nvq++, which targets the Quantum Intermediate Representation, a specification of a low-level machine language that quantum and classical computers can use to communicate. Researchers at Oak Ridge National Laboratory will be among the first to use this software.

These projects position NVIDIA strategically at classical and quantum inflection points, where classical advantage gives way to quantum value, according to Gartner Analyst Chirag Dekate.

Maybell Quantum exits stealth mode

Maybell Quantum exited stealth mode in March with the Icebox, a new design for quantum hardware. The founders have shrunk the cooling system required to run the specialized hardware down the size of a kitchen refrigerator. The Colorado company has more than a dozen patent-pending innovations, including Flexlines. These quantum wires offer "industry-leading performance and density, while transmitting a fraction of the heat and vibration of traditional cabling," according to the company. There are 4,500 of these wires in a single Icebox, which represents three items more qubits in one-tenth of the space, said Maybell's CTO Dr. Kyle Thompson.

New research center in Melbourne

Quantum Brilliance is planning a joint research and development hub with La Trobe University and RMIT University to develop high-performance, scalable diamond-based quantum microprocessors. The Research Hub for Diamond Quantum Materials will develop fabrication techniques.

Dr. Marcus Doherty is the co-founder and chief scientific officer of Quantum Brilliance, the head of

the Diamond Quantum Science and Technology Laboratory at the Australian National University and the leader of the Australian Army's quantum technology roadmap.

Professor Chris Pakes, acting deputy vice chancellor for research and industry engagement at La Trobe University, said the partnership will use both universities' expertise in diamond growth, surface imaging and engineering, and combine it with Quantum Brilliance's industry experience and manufacturing capabilities. Quantum Brilliance uses impurities within synthetic diamonds, and a carbon atom is swapped out for a nitrogen atom in the lattice of the crystal, to generate qubits.

Q-CTRL opens research institute

Q-CTRL is also supporting expanded quantum research through a partnership with The Paul Scherrer Institute. Dr. Cornelius Hempel, group lead for ion trap quantum computing at the university, said that efficient and automated tuneup and calibration procedures will be an essential aspect of day-to-day operations as quantum computers get larger and larger.

"Q-CTRL's hardware agnostic, yet hardware-aware tools will be very valuable in finding optimal control solutions that ensure uniform performance across larger qubit arrays," he said.

Both teams have experience in quantum computing based on trapped ions, including specialized approaches in error correction. The Institute has an existing research partnership with ETH Zurich via a quantum computing hub that opened in May 2021.

Agnostiq: Benchmarks should be application specific

SaaS startup Agnostiq has submitted a new research paper that recommends a more practical approach to measuring the progress of quantum computing: use benchmarks that match the application in question. Agnostiq conducted its research with a portfolio optimization task to determine whether quantum computers have actually improved over time for specific use cases.
The findings include:

One of the most significant findings was that high-quality portfolios were produced using quantum circuits requiring larger numbers of gates than previously demonstrated. This shows the quality of hardware for performing combinatorial optimization has improved because increasing the number of gates produces more noise, according to the researchers. Other findings include:

The peak solution quality was observed at higher depth (p=4) on 3 qubits on an IonQ trapped ion machine.

An IBM machine with the lowest qubit quality (quantum volume = 8) performed best of all the IBM machines tested.

Variability should be considered with all benchmarking numbers because quantum computers presently give variable results (as high as 29%) depending on the time the machines were accessed.

Agnostiq's Head of R&D Santosh Kumar Radha said the research was motivated by the fact that every

quantum hardware paradigm has its own set of performance metrics and each team is improving across different dimensions.

"We recognized a need to better understand how these non-trivial improvements translate to real-world applications." Radha said.

Agnostiq develops software tools that make quantum and high performance computing resources more accessible to enterprises and developers. Its open source workflow orchestration platform Covalent is designed to manage and execute tasks on heterogeneous compute resources.

28.OpenSSH Bravely Addresses The Quantum Threat

by Duncan Jones
https://medium.com/cambridge-quantum-computing/openssh-bravely-addresses-the-quantum-threat-86b03e38c2ba

OpenSSH has surprised and delighted the cyber world by switching to a hybrid post-quantum scheme in its latest 9.0 release. The software now uses a combination of Streamlined NTRU Prime, alongside old favourite X25519, to negotiate the session keys that protect data in transfer.

The release notes explain the rationale was to prevent "hack-now, decrypt-later" attacks, in which an attacker harvests encrypted data so they can hack it using a quantum computer in the future. Previous versions of OpenSSH were vulnerable to this type of attack because the algorithms used to negotiate encryption keys were based on mathematical problems that powerful quantum computers are expected to crack. Anyone sharing sensitive data across an OpenSSH connection was risking data exposure in 10 or 15 years when quantum computers increase in power. The Cloud Security Alliance argues this moment may come as soon as 2030.

The OpenSSH team should be applauded for taking a public stand at a time when most security products are in a holding pattern waiting for the NIST post-quantum process to complete. Although the timing of their release is surprising, with major NIST announcements expected in the days to come, it shows they value user security above the potential inconvenience of adjusting algorithms in subsequent releases.

What Is a Hybrid Crypto Scheme?

In a protocol like OpenSSH, data is encrypted using a session key known only to the sender and receiver. To securely exchange the session key, the sender and receiver perform a cryptographic handshake, which typically involves the use of quantum-vulnerable algorithms, such as RSA or ECDSA.

To defend against the quantum threat, a hybrid crypto scheme combines a quantum-vulnerable algorithm with a post-quantum algorithm to strengthen the cryptographic handshake. The resulting session

key is derived from mixing key material agreed by both algorithms. To gain access to the session key, an attacker would have to break the quantum-vulnerable algorithm as well as the post-quantum algorithm. This means the session key is likely to be safe from hack-now, decrypt-later attacks.

You might wonder what happens if the post-quantum algorithm is broken in the near future, as we saw recently with Rainbow. In such instances, the security of the connection collapses back to the security of the quantum-vulnerable algorithm. This means the data is perfectly safe against today's attackers, but potentially vulnerable to quantum attacks in the future. In short, you lose nothing by experimenting with hybrid approaches. In the worst case, you are no worse off, and in the best case, you are quantum-safe.

The main downside of hybrid approaches is that they haven't been broadly standardised yet. This means both the sender and receiver need to be aware of the bespoke combination of algorithms being used. In the OpenSSH example, both the client and the server need to be running OpenSSH 9.0 to negotiate a quantum-safe connection. If one end is running software from a different project (i.e. not OpenSSH) or an earlier version, the connection would still be quantum-vulnerable.

What Can We Learn from This?

Quantum presents both a threat and an opportunity to cybersecurity systems, and smart companies are exploring both sides of the coin today.

OpenSSH has reminded the world that little is lost by embracing quantum-safe algorithms in an aggressive manner, provided a hybrid approach is used. If you combine these algorithms with quantum-enhanced key generation, you can catapult to the cutting edge of connection security and feel confident you've taken every precaution available today.

Bravo to OpenSSH for getting the ball rolling. Hopefully, other security products are poised to implement quantum-safe algorithms as soon as the NIST announcements are made.

29.Indo-Israel Quantum Technology Collaboration with Military Focus

by Dr Ajey Lele

https://www.financialexpress.com/defence/indo-israel-quantum-technology-collaboration-with-military-focus/2485892/

Indian armed forces are doing dedicated investment in quantum technologies for some time now. During December 2021, Indian Army set up a Quantum Computing Laboratory at Mhow, Madhya Pradesh. This laboratory has been established with the help of the National Security Council Secretariat (NSCS). The purpose of this organisation is to carry out extensive research and development in the quantum field from a military perspective. This centre is facilitating research and training in the areas

like Quantum Key Distribution (QKD), quantum computing and quantum communication. And, their main focus is towards developing expertise in Quantum Cryptography, which is a mechanism to develop secure communications.

During April 5-6, 2022, a two-day Indo-Israel Bilateral workshop on Quantum Technologies (I2QT-2022) was held at New Delhi. This workshop was inaugurated by Dr G Satheesh Reddy, Chairman, Defence Research and Development (DRDO) and was jointly conducted by DRDO and IIT Delhi. The Israeli side was represented by their delegations consisting of academic experts, R&D professionals and Industry partners.

The DRDO workshop was one of the outcomes of the bilateral agreement (2021) signed amongst DRDO and Israel's Directorate of Defence Research & Development (DDR&D). Here the focus is towards promoting innovation and accelerating R&D in start-ups and Micro, small & Medium Enterprises (MSMEs) of both countries. It has been reported that the technologies developed under this collaboration will be available to both countries for their domestic applications. It is expected that this workshop would go a long way towards evolving a joint quantum technology roadmap. Such a roadmap would help identifying the exact military grade quantum technology specific domains for future collaborations.

From India's standpoint, it is very encouraging that DRDO has started investing in this technology at an early stage. This is because even today quantum sciences and many of their applications are still under process of evolution. Developments in the fields like quantum cryptography and quantum computing are found happening much faster than other fields. It is important for Indian agencies not to keep wasting time on reinventing the wheel in these arenas. Hence, collaborations with friendly states like Israel are going to be very useful.

From a defence utility perspective, quantum technologies show great promise. These technologies are expected to offer an alternative for space-based navigational systems like the GPS. Various other military related fields like submarine detection, radars and sensors are showing a lot of potential for applicability of quantum technologies.

Globally, the states like the US, China, Russia and Australia are found investing in quantum technologies. Presently, in their investments, military emphasis is found slowly getting more prominent. China (with assistance from Austria) has launched a quantum satellite. This satellite called Micius (launched during 2016) has successfully established an ultra-secure link between two ground stations separated by more than 1,000 km. China has surged ahead in the pursuit for unbreachable quantum communication and in future their defence forces are expected to gain largely from such innovations. Europe is working towards developing the Quantum Internet and so is the US and China. At present, it is difficult to conceptualise the exact military utility of such a system, but some defence agencies are working towards developing this new form of Internet with a view that such a system would be unhackable and would definitely emerge as a future military asset.

Israel started concentrating on the quantum domain around 2018. Their agencies like TELEM (National Centre for Research and Development) and MAFAT (Ministry of Defence) are mainly involved in undertaking research in various subfields of quantum sciences. Initially, during 2018, their overall investments were about USD27 million, but within two years, they have put in place a five year-plan of

about USD362 million. During Feb 2022, Israel's innovation and weapons research and development authorities have indicated the likely possibility of going for the first tender for building an Israeli quantum computer, as part of a massive project intended to give Israel "strategic capabilities". It would be a USD61.9 million project run by the Israel Innovation Authority and the weapons and technological infrastructure research body with help of industry.

India in its budget 2020, has announced a National Mission on Quantum Technologies & Applications (NM-QTA) with a total budget outlay of Rs 8000 crore for a period of five years. This budget is being utilised by the Department of Science & Technology (DST). The emphasis for investments includes quantum communication, quantum simulation, quantum computation and quantum sensing & metrology (science of measurement). Quantum technologies are dual-use technologies and hence at national level, DRDO needs to connect with DST. Some basic research and innovation could be done jointly by involving academic institutes like IITs.

Indian Space Research Organisation (ISRO) is also working on quantum sciences. DRDO can branch-off from such institutions, when they would be required to conduct exclusively defence related research, otherwise there is a need to utilise and collaborate with various national institutions (even the private sector) for conducting basic research in this field.

For defence technology collaboration, at bilateral level, India has an excellent relationship with Israel. During the recent bilateral workshop (I2QT-2022) there has been a wide-ranging deliberation on aspects like photonics-based quantum computing and communication, sensing, encryption, quantum magnetometry and atomic clocks. States like China are known to invest big in the field of quantum sciences and it is expected that in near future, PLA would derive various benefits from the ongoing research in this field. In this era of Industry 4.0, it is important for India's defence establishment to use various available resources to ensure that Indian armed forces benefit from the ongoing quantum revolution.

30.Tokyo Proposes First Domestic Quantum Computer Use by March 2023

by Kyodo
https://www.japantimes.co.jp/news/2022/04/07/business/tech/domestic-quantum-computer-plan/

The Japanese government intends to enter the global quantum computing race by putting its first domestically produced quantum computer into service within the current fiscal year ending March 2023, a source close to the matter said Thursday.

The new strategy includes plans to establish four quantum research centers across the country, and could be finalized later this month, the source said.

It comes after the ruling Liberal Democratic Party submitted proposals on March 24 to expand investment in quantum computing and other new technologies such as artificial intelligence.

The United States, China and other countries are in the middle of fierce competition over the development of quantum computing, which performs calculations by using the properties of quantum physics at the scale of atomic particles such as electrons and photons. It is expected to have a myriad of applications, including as a more efficient research tool for cryptography and the development of new medicines.

There are several proposed bases for quantum computing research — places to bolster the country's competitive edge and cultivate a workforce adept with the technology. The places proposed are Tohoku University, the Okinawa Institute of Science and Technology Graduate University, the National Institute of Advanced Industrial Science and Technology and the National Institutes for Quantum Science and Technology.

The government strategy aims to reach 10 million quantum technology users in Japan by 2030 and to create an environment where it can be used in such varied fields as medicine, banking and new materials development.

31.A Mathematical Shortcut for Determining Quantum Information Lifetimes

by Leah Hesla
https://www.anl.gov/article/a-mathematical-shortcut-for-determining-quantum-information-lifetimes

A new, elegant equation allows scientists to easily compute the quantum information lifetime of 12,000 different materials.

Scientists have uncovered a mathematical shortcut for calculating an all-important feature of quantum devices.

Having crunched the numbers on the quantum properties of 12,000 elements and compounds, researchers have published a new equation for approximating the length of time the materials can maintain quantum information, called "coherence time."

The elegant formula allows scientists to estimate the materials' coherence times in an instant — versus the hours or weeks it would take to calculate an exact value.

The team, comprising scientists at the U.S. Department of Energy's (DOE) Argonne National Laboratory, the University of Chicago, Tohoku University in Japan and Ajou University in Korea, published their result in April in the Proceedings of the National Academy of Sciences.

Their work is supported the Center for Novel Pathways to Quantum Coherence in Materials, an Energy Frontier Research Center funded by the U.S. Department of Energy, and by Q-NEXT, a DOE National Quantum Information Science Research Center led by Argonne.

The team's equation applies to a particular class of materials — those that can be used in devices called spin qubits.

"People have had to rely on complicated codes and calculations to predict spin qubit coherence times. But now people can compute the prediction by themselves instantaneously," said study co-author Shun Kanai of Tohoku University. "This opens opportunities for researchers to find the next generation of qubit materials by themselves."

Qubits are the fundamental unit of quantum information, the quantum version of classical computer bits. They come in different forms and varieties, including a type called the spin qubit. A spin qubit stores data in a material's spin — a quantum property inherent in all atomic and subatomic matter, such as electrons, atoms and groups of atoms.

Scientists expect that quantum technologies will be able to help improve our everyday lives. We may be able to send information over quantum communication networks that are impenetrable to hackers, or we could use quantum simulations to speed up drug delivery.

The realization of this potential will depend on having qubits that are stable enough — that have long enough coherence times — to store, process and send the information.

While the research team's equation gives only a rough prediction of a material's coherence time, it gets pretty close to the true value. And what the equation lacks in precision, it makes up for in convenience. It requires only five numbers — the values of five particular properties of the material in question — to get a solution. Plug them in, and voila! You have your coherence time.

Diamond and silicon carbide are currently the best-established materials for hosting spin qubits. Now scientists can explore other candidates without having to spend days calculating whether a material is worth a deeper dive.

"The equation is like a lens. It tells you, 'Look here, look at this material — it looks promising,'" said University of Chicago Professor and Argonne senior scientist Giulia Galli, a co-author of the study and Q-NEXT collaborator. "We are after new qubit platforms, new materials. Identifying mathematical relationships like this one points out new materials to try, to combine."

With this equation in hand, the researchers plan to boost the accuracy of their model.

They'll also connect with researchers who can create the materials with the most promising coherence times, testing whether they perform as well as the equation predicts. (The team has marked one success already: A scientist outside the team reported that the relatively long coherence time of a material called calcium tungstate performed as predicted by the team's formula.)

"Our results help us with advancing current quantum information technology, but that's not all," said Tohoku University Professor Hideo Ohno, who is currently president of the university and paper co-author. "It will unlock new possibilities by bridging the quantum technology with a variety of conventional systems, allowing us to make even greater progress with the materials we're already familiar

with. We're pushing more than one scientific frontier."

32.How to Make The Internet Secure in a Quantum World

by Grégoire Ribordy
https://www.forbes.com/sites/forbesbusinesscouncil/2022/04/07/how-to-make-the-internet-secure-in-a-quantum-world/?sh=5bc7042d1830

Governments worldwide are responsible not just for the physical security of their citizens but their digital security too. The private and public network infrastructure used by state-run institutions contains a wealth of sensitive, confidential and personally identifiable information. This makes it a very attractive proposition for any financially or ideologically motivated cybercriminal.

Big data requires big data security, which means protecting both the data itself and the networks across which it travels. The long-term value associated with much of this data means cybersecurity strategies need to provide protection not just against today's disclosed threats but tomorrow's emerging threat landscape.

Of course, government has a broader responsibility than simply keeping its own house in order. It has an essential role to play in the development and implementation of national cybersecurity standards. From breach notification legislation and data privacy laws to mandating zero-trust architecture for critical infrastructure, the remit is broad.

Meeting The 5G Security Challenge

The global roll-out of 5G networks has not been as smooth as some might have expected. Despite widespread acknowledgement that the fifth generation of cellular technology is essential for an effective IoT and big data world, implementation has been stymied by security concerns. Principal amongst these has been the potential for foreign states to use the infrastructure to eavesdrop on global communications. In the U.S., the FCC recently voted unanimously to "rip and replace" Huawei equipment at a cost of $1.9 billion.

While we think of 5G as a wireless technology, it is important to recognize that it is built on a fixed network of fiber optic cables. These high-speed networks that are the backbone of today's communications infrastructure have to be protected.

Securing The Network

Fiber tapping has been an effective eavesdropping tool since the networks were first deployed in the 1990s. The Snowden revelations in 2013 demonstrated the extent to which the NSA was exploiting fiber network vulnerabilities, a policy that appears to be alive and well today as evidenced by the re-

cent revelations in Denmark.

Effective use of high-speed networks is dependent upon trust: trust that the data is authentic and trust that it remains confidential. For the next generation of high-bandwidth networks, the question remains: how do you secure the network?

Public key cryptography is a vital weapon in the war against cybercrime, but it faces an unprecedented threat in the form of the quantum computer. Much has been written about the processing potential of quantum computers and how this could be a powerful tool for advancing the fields of statistical analysis, medical research and simulation. However, that same quantum computer processing power will render obsolete the public key cryptosystems we currently rely on to secure the internet. Clearly, this falls under the remit of long-term data protection and has become an area of focus for governments and corporations worldwide.

The Quantum Revolution

Quantum computers are not the only application of quantum technologies that will influence how we secure tomorrow's communication networks. In fact, some quantum applications have already been successfully commercialized and are helping to ensure the confidentiality and authenticity of data.

Encryption solutions are only as secure as the keys they use. The strength of the key is determined by the quality of entropy (randomness) used to generate it. Quantum random number generators (QRNG) are being used as a source of genuine entropy for key generation in applications ranging from core network infrastructure to mobile apps and IoT devices to create secure keys and help protect the authenticity and integrity of data.

Quantum key distribution (QKD) may represent the ultimate in long-term data protection as it delivers provably secure key exchange and confidentiality. It leverages a core principle of quantum physics that observation causes perturbation. In essence, this means any attempt to intercept or eavesdrop on the key transfer will cause transmission errors, which can be detected by legitimate users. At the end of the day, only valid secure keys are used, which ensures safe encryption and distribution of the data.

As the cloud goes quantum, one of the biggest markets will be the service sector, where QKD could be utilized to help secure financial transactions and data transmission.

An Investment In The Future Of Quantum

Those in the know are referring to the 2020s as the decade of quantum. Across the world, a broad range of quantum programs are underway. A recent report by CIFAR identifies 17 countries with an established quantum R&D strategy in place, with three others having a coherent strategy in development. These initiatives are designed to encourage the development of commercially viable applications of quantum technologies and are backed by significant levels of investment.

The CIFAR report estimates that worldwide funding of quantum has reached $22.5 billion, with China

leading the pack with a $10 billion investment. Europe also demonstrates a strong focus with $1 billion allocated to the Quantum Flagship initiative, as well as the upcoming EuroQCI initiative, which aims at deploying national quantum communication networks by 2027. The U.K. government has allocated over $1 billion to a multi-phase, 10-year strategy and in the U.S. the National Quantum Initiative Act approved $1.2 billion in spending across multiple departments.

Research is focused on three key areas of technology: quantum sensing, quantum communications and quantum computing. The CIFAR report highlights a near-term emphasis on quantum communications but also acknowledges that international governments have set their sights on the cybersecurity implications of the technology.

The quantum era is no longer a theoretical projection of a future technology state. With the commercialization of technologies like QRNG and QKD and the rapid development of the quantum internet, the future is now. Organizations must look into quantum security solutions (full disclosure: my company offers such solutions) to strengthen their current cryptosystems and provide instant, reliable, easy operation for both today's and tomorrow's data communications.

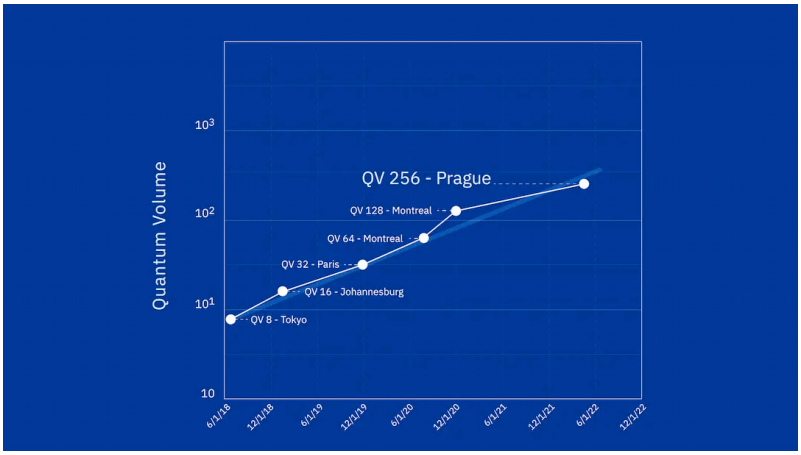
33.Pushing Quantum Performance Forward with Our Highest Quantum Volume Yet

by IBM

https://research.ibm.com/blog/quantum-volume-256

IBM Quantum has once again doubled the Quantum Volume of our highest-performing processor, achieving a Quantum Volume of 256 on the Falcon r10.

We previously stated that in order to achieve Quantum Advantage in the 2020s, we'd need to double the Quantum Volume of our processors every year. Well, we're excited to announce that we doubled it for the sixth time in five years with the latest announcement. Most importantly, this improvement joins a drumbeat of improvements across performance attributes as we work along our technology roadmap to bring about Quantum Advantage, sooner.



Quantum Volume is a measure of the largest square circuit of random two-qubit gates that a processor can successfully run. We measure success as the processor calculating the heavy outputs — the most likely outputs of the circuit — more than two thirds of the time with a 2σ confidence interval. If a processor can use eight qubits to successfully run a circuit with eight-time steps worth of gates, then we say it has a Quantum Volume of 256 — we raise 2 to the power of the number of qubits[1] (2^n) in order to demonstrate the size of the quantum state space the user has access to.

While the last two previous jumps in Quantum Volume have been attributed to improvements in our understanding of how to deal with coherent noise, plus better software and control electronics, reaching 256 was made possible thanks to a new processor which allows us to implement faster, higher-fidelity gates. Key to this advance was finding ways to reduce spectator errors, or those caused by calculations on qubits that are nearby, while still achieving faster two-qubit gates.

Thanks to these advances, we saw the bulk of our two-qubit gates approaching a 99.9% gate fidelity, meaning they would only err one in 1,000 times (though there were some outliers). And, we were still able to see strong coherence times despite performing the experiment on a new processor. When we ran the Quantum Volume experiment on eight qubits for eight time steps of random two-qubit gates, we measured heavy outputs an average of 68.5% of the time with a 2σ confidence high enough to successfully hit 256.

Scale. Quality. Speed.

Quantum Volume is how we measure the quality of our qubits. but we measure the performance of our quantum processors with three attributes: scale, quality, and speed. We push forward on scale by building larger processors; we measure speed with CLOPS[2], or circuit layer operations per second. Only through advancing on all of these fronts will we be able to bring about Quantum Advantage.

This announcement comes on the heels of our recent announcement of our largest quantum processor yet: our[3] 127-qubit Eagle processor. Thanks to our agile hardware development process, we've been able to push on scale, quality, and speed asynchronously, incorporating improvements into each new iteration of our hardware. We hope to soon incorporate our advances in Quantum Volume into larger systems, such as Eagle, to continue pushing forward on our hardware performance.

As always, we are following closely along our technology roadmap to constantly improve on all three of these fronts in order to bring about useful quantum computing as soon as we can.

---

[1] Note that n from Quantum Volume does not limit you to only n qubits with n time layers as demonstrated with several papers, such as "Error Mitigation for Universal Gates on Encoded Qubits," published in Physical Review Letters.

[2] Driving quantum performance: more qubits, higher Quantum Volume, and now a proper measure of speed with CLOPS.

[3] At the 2022 APS March Meetings, we presented an in-depth look into the technologies that allowed the team to scale to 127 qubits, and the benchmarks of the most recent Eagle revision.

34.The Side Effects of Quantum Error Correction and How to Cope with Them

by Andreas Trabesinger
https://www.phys.ethz.ch/news-and-events/d-phys-news/2022/04/the-side-effects-of-quantum-error-correction-and-how-to-cope-with-them.html

It is well established that quantum error correction can improve the performance of quantum sensors. But new theory work cautions that, unexpectedly, the approach can also give rise to inaccurate and misleading results — and shows how to rectify these shortcomings.

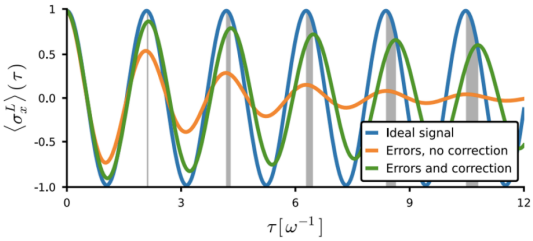
Quantum systems can interact with one another and with their surroundings in ways that are fundamentally different from those of their classical counterparts. In a quantum sensor, the particularities of these interactions are exploited to obtain characteristic information about the environment of the quantum system, for instance the strength of a magnetic and electric field in which it is immersed. Crucially, when such a device suitably harnesses the laws of quantum mechanics, then its sensitivity can surpass what is possible, even in principle, with conventional, classical technologies. Unfortunately, quantum sensors are exquisitely sensitive not only to the physical quantities of interest, but also to noise. One way to suppress these unwanted contributions is to apply schemes collectively known as quantum error correction (QEC). This approach is attracting considerable and increasing attention, as it might enable practical high- precision quantum sensors in a wider range of applications than is possible today. But the benefits of error- corrected quantum sensing come with major potential side effects, as a team led by Florentin Reiter, an Ambizione fellow of the Swiss National Science Foundation working in the group of Jonathan Home at the Institute for Quantum Electronics, has now found. Writing in Physical Review Letters, they report theoretical work in which they show that in realistic settings QEC can distort the output of quantum sensors and might even lead to unphysical results. But not all is lost — the researchers describe as well procedures how to restore the correct results.

Drifting off track

In applying QEC to quantum sensing, errors are repeatedly corrected as the sensor acquires information about the target quantity. As an analogy, imagine a car that keeps departing from the centre of the lane it travels in. In the ideal case, the drift is corrected by constant counter- steering. In the equivalent scenario for quantum sensing, it has been shown that by constant — or very frequent — error correction, the detrimental effects of noise can be suppressed completely, at least in principle. The story is rather different when, for practical reasons, the driver can perform correcting interventions with the steering wheel only at specific points in time. Then, as experience tells us, the sequence of driving ahead and making corrective movements has to be finely tuned. If the sequence would not matter, then the motorist could simply perform all steering manoeuvres at home in the garage and then confidently put the foot down on the accelerator. The reason why this does not work is that rotation and translation are not commutative — the order in which the actions of one type or

the other are executed changes the outcome.

For quantum sensors somewhat of a similar situation with non- commuting actions can arise, specifically for the 'sensing action' and the 'error action'. The former is described by the Hamilton operator of the sensor, the latter by error operators. Now, Ivan Rojkov, a doctoral researcher working at ETH with Reiter and collaborating with colleagues at the Massachusetts Institute of Technology (MIT), found that the sensor output experiences a systematic bias — or, 'drift' — when there is a delay between an error and its subsequent correction. Depending on the length of this delay time, the dynamics of the quantum system, which should ideally be governed by the Hamiltonian alone, becomes contaminated by interference by the error operators. The upshot is that during the delay the sensor typically acquires less information about the quantity of interest, such as a magnetic or electric field, compared to the situation in which no error had occurred. These different speeds in information acquisition then result in a distortion of the output (see the figure).



Sensical sensing

This QEC- induced bias matters. If unaccounted for, then for example estimates for the minimum signal that the quantum sensor can detect might end up being overly optimistic, as Rojkov et al. show. For experiments that push the limits of precision such wrong estimates are particularly deceptive. But the team also provides an escape route to overcome the bias. The amount of bias introduced by the finite- rate QEC can be calculated, and through appropriate measures be rectified in post- processing — so that the sensor output makes again perfect sense. Also, factoring in that the QEC can give rise to systematic bias can help to devise the ideal sensing protocol ahead of the measurement.

Given that the effect identified in this work is present in various common error- corrected quantum sensing schemes, these results are set to provide an import contribution to tweaking out the highest precision from a broad range or quantum sensors — and keep them on track to deliver on their promise of leading us into regimes that cannot be explored with classical sensors.

35.In Race to Build Quantum Computing Hardware, Silicon Begins to Shine

by Princeton University
https://phys.org/news/2022-04-quantum-hardware-silicon.html

Research conducted by Princeton University physicists is paving the way for the use of silicon-based

technologies in quantum computing, especially as quantum bits—the basic units of quantum computers. This research promises to accelerate the use of silicon technology as a viable alternative to other quantum computing technologies, such as superconductors or trapped ions.

In research published in the journal Science Advances, Princeton physicists used a two-qubit silicon quantum device to achieve an unprecedented level of fidelity. At above 99%, this is the highest fidelity thus far achieved for a two-qubit gate in a semiconductor and is on par with the best results achieved by competing technologies. Fidelity, which is a measure of a qubit's ability to perform error-free operations, is a key feature in the quest to develop practical and efficient quantum computing.

Researchers around the world are trying to figure out which technologies—such as superconducting qubits, trapped ions or silicon spin qubits, for example—can best be employed as the basic units of quantum computing. And, equally significant, researchers are exploring which technologies will have the ability to scale up most efficiently for commercial use.

"Silicon spin qubits are gaining momentum [in the field]," said Adam Mills, a graduate student in the Department of Physics at Princeton University and the lead author of the recently published study. "It's looking like a big year for silicon overall."

By using a silicon device called a double quantum dot, the Princeton researchers were able to capture two electrons and force them to interact. The spin state of each electron can be used as a qubit and the interaction between the electrons can entangle these qubits. This operation is crucial for quantum computation, and the research team, led by Jason Petta, the Eugene Higgins Professor of Physics at Princeton, was able to perform this entangling operation at a fidelity level exceeding 99.8 percent.

A qubit, in simplest terms, is a quantum version of a computer bit, which is the smallest unit of data in a computer. Like its classical counterpart, the qubit is encoded with information that can have the value of either one or zero. But unlike the bit, the qubit is able to exploit the concepts of quantum mechanics so that it can perform tasks classical bits cannot.

"In a qubit you can encode zeros and ones, but you can also have superpositions of these zeros and ones," said Mills. This means that each qubit can be simultaneously a zero and a one. This concept, called superposition, is a fundamental quality of quantum mechanics and one that allows qubits to do operations that seem amazing and otherworldly. In practical terms, it allows the quantum computer a greater advantage over conventional computers in, for example, factoring very large numbers or isolating the most optimal solution to a problem.

The "spin" in spin qubits is the electron's angular momentum. It is a quantum property that manifests as a tiny magnetic dipole that can be used to encode information. A classical analog is a compass needle, which has north and south poles, and rotates to align with Earth's magnetic field. Quantum mechanically, the spin of the electron can align with the magnetic field generated in the lab (spin-up), or be oriented anti-parallel to the field (spin-down), or be in a quantum superposition of spin-up and spin-down. Spin is the property of the electron harnessed in silicon-based quantum devices; conventional computers, by contrast, work by manipulating an electron's negative charge.

Mills asserted that in general, silicon spin qubits have advantages over other qubit types. "The idea is

that every system is going to have to scale up to many qubits," he said. "And right now, the other qubit systems have real physical limitations to scalability. Size could be a real problem with these systems. There's only so much space you can cram these things into."

In comparison, silicon spin qubits are made from single electrons and are extremely small.

"Our devices are just about 100 nanometers across, while a conventional superconducting qubit is more like 300 microns across, so if you want to make many on a chip, it's going to be difficult using a superconducting approach," Petta said.

The other advantage of silicon spin qubits, Petta added, is that conventional electronics today are based on silicon technology. "Our feeling is that if you really want to make a million or ten million qubits that are going to be required to do something practical, that's only going to happen in a solid-state system that can be scaled using the standard semiconductor fabrication industry."

Still, operating spin qubits—like other types of qubits—with a high fidelity has been a challenge for researchers.

"One of the bottlenecks for the technology of spin qubits is that the two-qubit gate fidelity up until very recently has not been that high," Petta said. "It's been well below 90 percent in most experiments."

But it was a challenge that Petta and Mills and the research team believed could be achieved.

To perform the experiment, the researchers first had to capture a single electron—no small task.

"We're trapping a single electron, a very small particle, and we need to get it into a specific region of space and then make it dance," said Petta.

To do this, Mills, Petta and their colleagues needed to construct a "cage." This took the form of a wafer-thin semiconductor made primarily out of silicon. At the top of this the team patterned little electrodes, which creates the electrostatic potential used to corral the electron. Two of these cages put together, separated by a barrier, or gate, constituted the double quantum dot.

"We have two spins sitting in adjacent sites next to each other," said Petta. "By adjusting the voltage on these gates, we can momentarily push the electrons together and cause them to interact. This is called a two-qubit gate."

The interaction causes each spin qubit to evolve according to the state of its neighboring spin qubits, which leads to entanglement in quantum systems. The researchers were able to perform this two-qubit interaction with a fidelity exceeding 99 percent. To date, this is the highest fidelity for a two-qubit gate that has thus far been achieved in spin qubits.

Petta said that the results of this experiment place this technology—silicon spin qubits—on an equal footing with the best results achieved by the other major competing technologies. "This technology is on a strongly increasing slope," he said, "and I think it's just a matter of time before it overtakes the

superconducting systems."

"Another important aspect of this paper," Petta added, "is that it's not just a demonstration of a high fidelity two-qubit gate, but this device does it all. This is the first demonstration of a semiconductor spin qubit system where we have integrated performance of the entire system—the state preparation, the read out, the single qubit control, the two-qubit control—all with performance metrics that exceed the threshold you need to make a larger-scale system work."

In addition to Mills and Petta, the work also included the efforts of Princeton graduate students Charles Guinn and Mayer Feldman, as well as University of Pennsylvania assistant professor of electrical engineering Anthony Sigillito. Also contributing to the paper and research were Michael Gullans, Department of Physics, Princeton University and the Center for Quantum Information and Computer Science at NIST/University of Maryland, and Erik Nielsen of the Sandia National Laboratories, Albuquerque, New Mexico.

36.Outgunning The Us, China Looks at Gaining Unassailable Lead in Quantum Tech with New Helium Cooling System

by EurAsian Times Desk
https://eurasiantimes.com/china-looks-at-gaining-lead-in-quantum-tech-with-new-helium/

China is striving to become a world leader in quantum technology through its national strategy of innovation-driven development. Last week, a team of researchers from Shanghai claimed to have developed a novel cooling system to create extremely low temperatures needed for quantum computers to function.

The core components of most quantum machines – from computers to satellites – detect and manipulate subatomic particles that are easily disturbed by heat to store and process information and therefore these machines need to operate in conditions near absolute zero.

To maintain the 'quantum state' of a system it is essential to minimize the risk of anything disrupting the fragile position, such as the slightest increase in temperature can cause the atoms and molecules to move around too much and increase the voltage of subatomic particles inside them thereby changing their quantum state.

Helium-3 — Extremely Rare On Earth

Cooling the most advanced quantum hardware requires helium-3, an isotope of helium that has an unmatched level of efficiency in carrying away the heat. However, Helium-3 is extremely rare on Earth and the main supply comes from the aging nuclear warheads.

In less than two decades, Helium-3 has seen an exponential rise in its demand for quantum research and other disruptive technology and its price has increased more than 40-fold to over $5,000 per liter in gas form.

Furthermore, not anybody can just buy it. For example, in the US Helium-3 is one of the few commodities that are subject to strict government production and distribution controls on military grounds.

In a paper published last week in a domestic peer-reviewed Science Bulletin, Professor Dang Haizheng and his colleagues with the Shanghai Institute of Technical Physics at the Chinese Academy of Sciences said that they had built a powerful cooling system for some of the most demanding quantum machines without using any Helium-3 at all.

Helium-4 The Super Fluid

This new cooling device makes use of Helium-4, another helium isotope that is used as a gas for party balloons. Helium-4 is much more abundant than Helium-3 but is less effective as a coolant in extreme conditions

Helium-4 when subjected to temperatures as low as 2 kelvin (-271 degrees Celsius), turns into a superfluid, climbing walls regardless of gravity and becoming much more difficult to control.

A superfluid can do things that no other fluid can, which is to defy the laws of gravity and climb the walls of a container and escape.

Dang's team has developed a theoretical model that could predict the behavior of Helium-4 flow in a superfluid state to some extent.

The cooling system they built has a working principle similar to a household refrigerator but has few moving parts. It is driven by a pulse energy source and operates at a high frequency to increase heat-transfer efficiency.

To contain Helium-4's irregular behavior, Dang's team has added a special component to stop the anti-gravity climb. Part of the device must also be built with extremely high-quality components with precision twice as high as mainstream products today, according to the researchers.

In their experiment, the new cooling device kept a superconducting nanowire single-photon detector, an optical sensor commonly used in quantum machines, at a temperature of 1.8 kelvin for more than two weeks (15 days).

The results of this experiment showed that Helium-4 has the potential to replace Helium-3 completely in some of the most demanding applications such as space missions, the researchers claimed.

"This is great news," said a quantum physicist in Hefei, Anhui province, who declined to be named.

Finding a Helium-3 substitute could reduce the cost of quantum technology in radars by at least 10 percent, according to the researcher's rough estimate.

In 2016, a team of Chinese researchers from China Electronics Technology Group Corporation's 14th Research Institute's Key Laboratory of Intelligent Sensing Technologies claimed to have developed a 'quantum radar' that could detect targets up to 100 km.

The Chinese media at the time dubbed this radar, the "nemesis" of stealth fighter jets. The lead researcher said that the system will track not only stealth aircraft but also "high-speed flying objects in the upper atmosphere and above" — that is, ballistic missiles.

Mass Application of Quantum Technology

Apart from that some of the most significant contributions of China to the development of quantum technology include the world's first quantum satellite, the longest quantum communication network and the fastest quantum computers.

However, all of the above were developed using sensors cooled by Helium-3 and the use of Helium-4 could further enable the mass application of quantum technology.

That said, the viability of the new cooling device is questionable because the experiment was conducted in a laboratory.

What is important though, is that once dismissed as a copycat of foreign developed technologies, China is leading the way in innovations related to emerging technologies such as quantum technology.

China should be a "global leader in innovation" by 2035, President Xi Jinping declared during the Chinese Communist Party's 19th National Congress last October.

Under its 13th five-year plan, China has launched a "megaproject" for quantum communications and computing, which aims to realize major breakthroughs in these technologies by 2030, including the expansion of China's national quantum communications infrastructure, the development of a general quantum computer prototype, and the construction of a practical quantum simulator.

37.Microsoft Announces New Windows 11 Security, Encryption Features

by Sergiu Gatlan

https://www.bleepingcomputer.com/news/microsoft/microsoft-announces-new-windows-11-security-encryption-features/

Microsoft says that Windows 11 will get more security improvements in upcoming releases, which will add more protection against cybersecurity threats, offer better encryption, and block malicious apps

and drivers.

"In a future release of Windows 11 you're going to see significant security updates that add even more protection from the chip to the cloud by combining modern hardware and software," said David Weston, VP for Enterprise & OS Security.

One of the new security features Microsoft is adding in Windows 11 is **enhanced phishing protection** against targeted phishing attacks with the help of Microsoft Defender SmartScreen, a cloud-based anti-phishing and anti-malware service.

With SmartScreen integrated into the OS, Windows users will be warned when entering their credentials into malicious applications or hacked websites.

As proof of SmartScreen's efficiency, Weston said Microsoft has blocked over 25.6 billion Azure Active Directory brute force authentication attacks and was able to intercept more than 35.7 billion phishing emails before landing in the recipients' inboxes just in the last year alone.

"These enhancements will make Windows the world's first operating system with phishing safeguards built directly into the platform and shipped out of the box to help users stay productive and secure without having to learn to be their own IT department," he added.

Protection for user data and against malicious drivers

Weston also said Windows 11 users would get additional layers of security that protect their data and act as a defense against malicious drivers.

The newly planned **Personal Data Encryption** feature, for instance, protects users' files and data when they are not signed into the device by blocking access until they authenticate via Windows Hello.

"To access the data, the user must first authenticate with Windows Hello for Business, linking data encryption keys with the user's passwordless credentials so even if a device is lost or stolen, data is more resistant to attack and sensitive data has another layer of protection built in," Weston said.

Windows 11 customers will also be able to enable a **vulnerable driver blocklist** that uses Windows Defender Application Control (WDAC) to block drivers with known vulnerabilities automatically.

It hardens Windows systems against third party-developed drivers with any of the following attributes:

Known security vulnerabilities that attackers can exploit to elevate privileges in the Windows kernel

Malicious behaviors (malware) or certificates used to sign malware

Behaviors that are not malicious but circumvent the Windows Security Model and can be exploited by attackers to elevate privileges in the Windows kernel

Windows 11 app, enterprise security improvements

Smart App Control is another crucial security enhancement planned for Windows 11 that will be integrated with the OS at the process level to block users from running malicious apps using code signing coupled with an AI model.

"When a new application is run on Windows 11, its core signing and core features are checked against this model, ensuring only known safe applications are allowed to run," Weston added.

"This means Windows 11 users can be confident they are using only safe and reliable applications on their new Windows devices."

Microsoft also wants to enable Credential Guard by Default and additional protection for Local Security Authority (LSA) for organizations using Windows 11 Enterprise to improve security in enterprise environments further.

The company's engineers have also added other security enhancements to secure Windows 11 users' accounts, devices, and apps since this new version's release in October 2021.

Probably the most important of them, named Config Lock, locks security settings to have them automatically reverted if end-users or attackers try to modify them.

It utilizes MDM policies to monitor and revert registry keys to the original states if users are altering them, likely rendering their devices insecure and exposed to attacks.

38.In Cybersecurity, Strengthening Encryption is Vital

by Denis Mandich

https://www.forbes.com/sites/forbestechcouncil/2022/04/04/in-cybersecurity-strengthening-encryption-is-vital/?sh=37d78af52394

Complex systems can break in complex ways. However, this statement is not easily quantified in cybersecurity, where it is better rephrased: "With each layer of software integration, a system inches closer to disaster." This is counterintuitive because these tools are promoted as improvements. More automation, virtualization and other enhancements lead to more interdependencies, where single issues can lead to cascading failure. Encryption is at the foundation of almost every cybersecurity technology from MFA to firewalls and HTTPS. Ironically, it is also the essential component of ransomware.

While dissecting the different complexities leading to disaster is enlightening, starting at the foundations is critical to improving outcomes. These are the deepest and most pervasive risks with disproportionate impact. Poorly implemented cryptographic algorithms can frequently infect applications that are otherwise secured with additional protections. The result is massive data leaks, enduring vulnera-

bilities and penetrated networks. A few recent examples are a great reminder that any size company can be affected.

Samsung's Galaxy flaw impacted 100 million phones and was traced to the first step in any crypto operation—generate a random number for a key. When the first step is weak, easily compromised or broken, the security guarantees further up the food chain are invalidated. The developers were not cryptographers and likely had no idea that their proprietary implementation was deeply flawed. They suffered from the common delusion that "security by obscurity" was a solution and a black box inside their software was protection in and of itself.

If a new bulletproof vest was never tested with real ammo, would any soldier use it? There are long-studied and proven methodologies in almost any industry to prevent manufacturing disasters, but there are few in cybersecurity. Recommended best practices are frequently discarded for expediency, but that would never be tolerated for pharmaceuticals or vehicles.

As more devices and systems like critical infrastructure get connected to the internet, the problem grows exponentially while becoming more difficult to check. A very similar randomness flaw can be found in billions of IoT devices that were not built to use or handle high-security applications. Instead of large random numbers for keys, all zeros or the number one were generated. Obviously, this is very easy to guess and check for millions of devices at once but difficult to discover buried inside a complex industrial system like the power grid or petroleum distribution networks. Basic encryption is one of several complicated, specialized and deep subsystems that are easy to get wrong. On the surface, individual devices and networks may have the illusion of invulnerable security, but insidious defects are lurking.

We're accelerating toward a society that's always on and always tethered to the internet, with the increasing likelihood that AI will be essential to securing daily life. There is no historical precedent to prove this will work well and not accelerate us to a cyber black swan event. Stanislav Petrov prevented a nuclear war when he realized a Soviet nuclear warning system was giving him false information about a U.S. nuclear attack. Against all military doctrine and protocol, he unilaterally decided not to launch an apocalyptic counterstrike. Can AI running a wired planet prevent cyber warfare targeting transportation, energy, banking and our digital way of life?

Cybersecurity has evolved from an enterprise afterthought or costly burden to a critical interest of the board. Durable solutions address specific vulnerabilities, but many are unknown before a breach is discovered. Attackers will get inside any network to perform reconnaissance before prioritizing collection. Encryption, deployed correctly, can prevent a contagion from probing and spreading. The goal must be to minimize the impact by encrypting all data-at-rest with strong user controls and creating end-to-end encryption (E2E) channels for application data-in-motion. This can transform an enterprise from a college campus data free-for-all to a responsible participant in national economic security. In a virtualized business world with remote employees using the open internet, a secure parking lot and building turnstile are part of the security theater.

The quantum computing age ushers in a new era that's vastly different from all human history. For comparison, to a quantum computer with a few thousand logical qubits, the difference in the computing power of an abacus to all of the supercomputers in existence is zero. Why? Quantum computers

can solve problems that are otherwise impossible, regardless of the size of a classical supercomputer. Transitioning to quantum secure solutions will be challenging because older systems will need to be replaced, not updated. New software will have to be crypto-agile, meaning that algorithms must be treated as temporary and easily swappable, or they will become quickly obsolete and irreparable. The process will take years, so starting now is essential. Getting it right means doing it cleanly and efficiently, unbundled from the Swiss Army knife cyber tools.

Data is rarely "stolen"; there's just a copy of it on a foreign server waiting to be operationalized. You still have it, unlike a stolen laptop. If it was strongly encrypted and secured with post-quantum cryptography (PQC), the threat is no longer existential. Even the best nation-state hackers will be unable to use most, if any, of it. Cyber insurance, board reporting requirements, and shareholder and customer notifications will have policies accounting for quantum safety or classical weakness. A good measure of confidence is posting the encrypted data in a public forum as an operational test for developers.

Isolating systems and reducing complexity can walk security backward from the edge of catastrophe.

39.10 Difficult Problems Quantum Computers Can Solve Easily

by Apoorva Bellapu
https://www.analyticsinsight.net/10-difficult-problems-quantum-computers-can-solve-easily/

Quantum computing is on its way to being considered one of the most innovative technologies. Not only is this form of computing a better replacement for classical computing but also a potential complement for a specific set of applications. Considering how important quantum computing has become over a period of time, today it has reached a stage where it has the potential to solve a significant number of problems. On that note, have a look at 10 difficult problems quantum computers can solve easily.

Quantum encryption

Considering how intercepting the data would corrupt the communication, can anything get better than securing communication from interception or eavesdropping? Well, quantum encryption has to its rescue. With this in place, the person disrupting the particle cannot get usable information, and the recipient can be alerted to the eavesdropping attempt.

Simulation of quantum systems

What cannot go unnoticed, is the fact that even if a few qubits of quantum systems are to simulate, it'd be extremely expensive when it comes to the resources required. This is where quantum computing serves to be no less than a blessing.

ab initio calculations

Classical computing is of very little help when the task to be accomplished pertains to ab initio calculations. With quantum computing in place, you have a quantum system simulating another quantum system. Furthermore, tasks such as modelling atomic bonding or estimating electron orbital overlaps can be done much more precisely.

Solving difficult combinatorics problems

Yet another difficult area that quantum computers cater to is that of solving difficult combinatorics problems. The algorithms within quantum computing aim at solving difficult combinatorics problems in graph theory, number theory, and statistics. Well, the list is likely to continue in the near future.

Supply chain logistics

Logistics is more or less related to a set of problems that cannot be solved using a brute force algorithm. Rather than meeting the set objectives via numerous individual operations, quantum computers do it in the easiest manner possible.

Optimization

One of the most difficult problems that quantum computers can solve is – "optimization". One major aspect of this includes determining optimal weights for neural nets, so a classifier would be as good as it can be on a set of training data.

Finance

Economics is associated with numerous sophisticated models of market behaviour in the hope of predicting important and disruptive events. With quantum computing, we can now process and retrieve data from incredibly large data sets and make predictions about markets that can have an outsized global impact.

Drug development

The drug industry, without a doubt, has a lot of experimentation and discovery happening at the back end. This is not only time-consuming but also expensive. A quantum computer, on the other hand, can process all the variables concurrently and will greatly reduce the time and cost necessary to develop new drugs.

Data analysis

The growing data is posed as one of the biggest challenges for classical computing. This is where quantum computing came into play. Quantum computers have the ability to process large data sets in

record time.

Weather forecasting

With many environmental variables in place, it becomes quite difficult for classical computers to forecast weather. However, a quantum computer can not only forecast near-term weather patterns well but also predict the effect of climate change.

40.How Is China Educating A Quantum Workforce?

by Amara Graps
https://quantumcomputingreport.com/how-is-china-educating-a-quantum-workforce/

With China's tremendous quantum funding through its departments: MOST (Ministry of Science and Technology) and the NDRC (National Development and Reform Commission), what about the quantum mandates that reach the youth? Does quantum education in the public school system exist? Yes, it does, with new initiatives.

Primary Education Modernization

From top to bottom, there is a push to include quantum technology in primary grades as part of the country's education modernization plans. Chen Yunlong, the deputy director of the Basic Education Curriculum and Textbook Development Center of the Ministry of Education writes that "The future has come, and the strides of basic education should also keep up with the wave of technological development," after mentioning specifically artificial intelligence, big data, **quantum information**, and biotechnology. For that future, China has issued two documents: "China's Education Modernization 2035" and "The Implementation Plan for Accelerating the Promotion of Educational Modernization (2018-2022)" accelerating the modernization of education. The year of 2035 is of special importance in China's overall development timetable, as the country has pledged to realize socialist modernization by then.

The modernization plan aims to open the curriculum of primary and secondary schools, to encourage children to explore their interests, and to expand curricula with interactive science and technology. The money that China is investing in their educational improvement is considerable.

In the first year, 2019, of China's Education Modernization 2035 plan, they allocated more than 4 percent of GDP, and more than one trillion yuan ($157 billion). Since I am limited to open sources, we can see that such funding must be widely distributed. For example, in MOST's 2020 final budget, the education line item is 1,212,100,000 yuan = $191 Million. With such funding, and with this new framework, there is a funding and policy support for quantum education to enter the primary and secondary schools. Some recent examples of quantum education of the youth in practice can be seen

by Quantum Origin and CIQTEK, below.

Hefei Quantum Companies Support Quantum Education

In September 2017, Origin Quantum Computing Technology Co., Ltd., (合肥本源量子计算科技有限责任公司 translated as 'Yuanyuan' Quantum or 'Benyuan' Quantum), China's first quantum computing startup, was established. Today it is a 300-employee company in Hefei. To promote the development of quantum computing and cultivate domestic quantum computing talents, Origin Quantum opened a quantum education section of the company, while developing its quantum computing software and hardware systems.

In 2021, Origin Quantum visited Hefei Normal Primary School. From the Founders' educational roots at University of Science and Technology of China, Guo Guoping explained 'What is quantum, what is quantum computing, and what does a quantum computer look like?' to students.

School visits are only one part of its education efforts. The company has cloud-based quantum educational hardware: the Yuanyuan Quantum Learning System, as well.

Another Hefei-based quantum technology company: CIQTEK has an intriguing quantum computing educational device based on nitrogen-vacancy (NV) center in diamond, but few details are provided and no price is listed.

University Quantum Education

The "Implementation Plan described above" proposes ten key tasks to promote the modernization of education; the fourth task is what I will address in the context of quantum education and research.

In the implementation plan, higher education reform is spelled out: the development of a new double first-class network of universities, high level post graduate education, training of rare, high-value skills, improvement of scientific research, construction of cutting edge science centers, and participation in national laboratory construction.

University of Science and Technology of China (USTC): Quantum Technology Education Leader

As early as the 1990s, (USTC) offered quantum-related elective courses such as quantum for graduate students. Later, related elective courses were also offered for undergraduates. However, quantum information science's interdisciplinary nature, between informatics and quantum physics needs its own undergraduate and graduate category. The senior academicians agree on the need to build a young quantum-educated workforce. Chinese Academy of Sciences quantum Professor Guo Guoping: "to realize the related tasks in the field of **quantum information** in the 14th FYP, it is necessary to have a sufficient scale of outstanding young talents to support. " Guoping's wish was realized in 2021.

2021: New Quantum Information Science Majors

Early in 2021, the Ministry of Education announced the results of the 2020 filing and approval of **undergraduate majors** in general institutions of higher learning. Thirty-seven new majors were included in the catalogue of undergraduate majors in ordinary colleges and universities of which **quantum information science** is one. "The addition of an undergraduate major in quantum information science is timely and necessary, and it also reflects the country's commitment to the quantum technology industry," said Guo Guoping. Several universities started their quantum information undergraduate coursework. The University of Science and Technology of China (hereinafter referred to as USTC) was one. Tsinghua University was another.

Postgraduate quantum information courses are offered too: In addition to USTC, where quantum courses have long been available in masters and doctoral studies, Guo Guoping says that Shanxi University, Institute of Physics, Chinese Academy of Sciences and other units in China are also offering postgraduate courses in quantum information science, as well as many domestic colleges and universities with similar elective courses.

Quantum Skills Growth and Future Quantum Hotbeds

With China's enormous education support, the soon-to-be-degreed quantum information students will be making their mark in the world. See the pool of Engineering graduate students in the line item on the next figure from the Ministry of Education 2020 statistics. These **250282** graduate students of a variety of engineering skillsets are a vector into the future pool of quantum technology in the country.

How far has China come in this education implementation plan for quantum technology? Let's choose one sector where China's skills are strong: **quantum dots**. Of the quantum dot patents granted since 2016, the institutions of those patents comprise 20% of the list of double first-class institutions announced in February 2022 by the Chinese Ministry of Education. This initiative, therefore, is still early and needs more time. The quantum research progress up to now has still been **more dependent on the groups of quantum mentors and quantum leaders**. However, I suggest you to keep your eye on the map of country's double first-class institutions for future quantum research hotbeds.

Quantum Information Science Integration with Industry

In Guoping's view, training talents majoring in quantum information science should pay more attention to the traction and integration of the industry. "For example, we ask students from the School of Finance to take courses in quantum information, and he will apply quantum computing to the financial field in the future," he says.

A step in the education-industry integration direction can be seen at the provincial level with the January 2022 news, that the "Industry-Education Integration Promotion Association" of the Guangdong province will assist and guide schools and enterprises to jointly build 50 industry-education integration projects. Such examples highlight the deeply woven character of government policy implementation from top to bottom.

Recruitment

The Chinese government initiated the Thousand Talents Plan (TTP) in 2008, with the goal of making China the world's leader in science and technology by 2050. As a way to bring leading Chinese scientists, academics and entrepreneurs living abroad back to China with their acquired skills, it served as an effective strategy to build technology teams that could serve as teachers and industry leaders. In 2011, the scheme grew to encompass younger talent and foreign scientists. Until the TTP was rebranded in 2020, due to US intellectual property concerns, to the High-End Foreign Expert Recruitment Plan, it attracted more than 7,000 scientists including the well-known quantum scientist Jian-Wei Pan. If a Chinese student today is interested to study abroad, they have additional support from the Industrial and Commercial Bank of China: an 'easy loan': 2 Million RMB, which is about 300K USD. Kania and Costello, 2018 describe how many leading Chinese quantum physicists become key figures in Chinese quantum science and technology after receiving PhDs from and pursuing research at top U.S. and international institutions.

41.What Is Quantum Computing? Why Should I Be Concerned?

by CSA Quantum-Safe Security Working Group
https://cloudsecurityalliance.org/blog/2022/04/02/what-is-quantum-computing-why-should-i-be-concerned/?utm_source=Email

What is quantum mechanics?

Quantum mechanics/physics is a long-proven physical science that describes actions and properties of very small particles. Everything in the universe works and depends on quantum mechanics. It's how the world works. Computers and software are being created that function using quantum particles and properties. Within a few years, if not already, we will have quantum computers capable of doing things non-quantum computers cannot, including breaking many forms of traditional cryptography and creating new, unbreakable forms of cryptography.

How long have quantum computers been around?

The first working quantum computer was created in 1998. Today there are hundreds of fairly crude quantum computers and hundreds of different types of quantum devices. All known quantum computers are still relatively weak and are in the laboratory and experimental stages, but are predicted to become stronger as time goes on. The world's governments and corporations are spending billions of dollars a year in the pursuit of building quantum supercomputers and networks. Quantum computer vendors include the world's largest companies, such as Google, IBM, Intel, Microsoft, and Alibaba.

How is quantum computing able to threaten traditional cryptography?

Particular types of quantum computers, armed with a mathematical algorithm known as Shor's algo-

rithm, can quickly factor math equations that involve large prime numbers. Equations involving large prime numbers are what give most traditional public key cryptography its protective capabilities. Traditional binary-based computers cannot easily factor large prime number equations. Quantum computers with enough "qubits" can factor large prime number equations in a very short amount of time, measured in minutes to days.

When will quantum computers break traditional public key cryptography?

No one knows for sure, although as soon as quantum computers get four thousand or so "stable" or usable qubits, or that computational equivalent, it is believed that traditional public keys 2048-bits long or shorter will be quickly crackable. Most of the world's existing public cryptography relies on such keys. Quantum computers are capable of weakening the protective power of other types of cryptography as well, such as symmetric key cryptography.

General estimates of time until quantum computers are capable of breaking traditional public crypto range from a few years to over ten years. **CSA estimates that on April 14, 2030, a quantum computer will be able to break present-day cybersecurity infrastructure.** We're calling this pending threat Y2Q.

Regardless of the specific date, most experts and the US government say now is the time to start preparing. If the break happens sooner than people are expecting, then we will be better prepared to respond appropriately. Take the first step by learning more about the quantum threat. In this recording from the CSA Research Summit, hear first-hand from one of the CSA Quantum Working Group leaders about this threat and what we as an industry can do to prepare. You can also learn more by downloading and reading our paper, Practical Preparations for the Post-Quantum World.

42.DARPA Awards Contracts for The Quantum Benchmarking Program

https://quantumcomputingreport.com/darpa-awards-contracts-for-the-quantum-benchmarking-program/

In April 2021, we reported that the U.S. Defense Advanced Research Projects Agency (DARPA) had announced funding opportunities were available for a Quantum Benchmarking program and was soliciting proposals for it. The program has goals to create new benchmarks that quantitatively measure progress towards specific computational challenges and also attempt to define the computer hardware necessary to measure benchmark performance. It has now announced that it is awarded contracts to Raytheon BBN, University of Southern California (USC), and a team of five organizations including Aalto University, IonQ, University of Technology Sydney, University of Texas at Dallas, and Zapata Computing. The Raytheon BBN contract was for $2.9 million, the USC contract was for $4.1 million, and the amount for the five member team has not yet been announced. Additional information about the Raytheon BBN and USC awards is available here and a news release from Zapata about their participation in the award can be found here.

43.Entrust on The Future of A Post-Quantum Security Landscape

by Alex Tuck
https://technologymagazine.com/cloud-and-cybersecurity/Entrust-on-the-future-of-a-post-quantum-security-landscape

Quantum computing is expected to disrupt encryption based cryptographic defense by 2030, according to IT security specialists Entrust.

Entrust formed in 1969, with the founding of Datacard Corporation and the advent of secure, high-speed payment and identity card printers. Since then, they have acquired other powerful brands, developed new technologies, and extended their global footprint. Their vision is built around 'Securing a world in motion'.

In a recent industry roundtable, Anudeep Parhar, Chief Information Officer & General Manager PKI and IoT Solutions BU at Entrust Datacard, and Greg Wetmore, Vice President Product Development at Entrust, explained how quantum computing will augment classic computing, as opposed to replacing it.

This post-quantum world will be hybrid, spanning decades and industries with high privacy and compliance obligations will lead with most vulnerable use cases.

According to nCipher Chief of Security, Dr. Pali Surdhar, "The National Institute of Standards and Technology (NIST) is working to identify the best quantum-safe algorithms that are less likely to be broken by quantum techniques. That includes the creation of algorithms that are based on symmetric and hash-based schemes or using other approaches, such as code-based, lattice-based and multivariate cryptography."

What is Quantum Computing?

According to Anudeep Parhar, quantum computing is "an area of computing focused on developing computer technology based on the principles of quantum theory, which explains the behaviour of energy and material on the atomic and subatomic levels."

As classic computers can only encode information in bits that take the value of 1 or 0, this restricts their ability, whereas quantum computing uses quantum bits or qubits, therefore harnessing the unique ability of subatomic participles that allows them to exist in more than one state i.e., a 1 and a 0 at the same time.

Superposition and Entanglement are two quantum physics concepts leveraged by these supercomputers, according to Parhar.

"This empowers quantum computers to handle operations at speeds exponentially higher than conventional computers and at much lesser energy consumption. Post-quantum cryptography is the development of new kinds of cryptographic approaches that can be implemented using today's classical computers but will be impervious to attacks from tomorrow's quantum ones," said Parhar.

Post quantum cryptography and its impact on business

Parhar adds that the movement of data across the internet today is secured by public key encryption algorithms

"Quantum computers can break current public key encryption. Mitigation strategies are required now to address this business risk. Information that needs to be secure in 5 years or more needs to be protected now," he said.

Greg Wetmore is Vice President Product Development at Entrust. Talking of a fragmented quantum community, Wetmore said that "when it comes to PQ standards, NIST is at the centre. At this stage of maturity, NIST has acknowledged the need for hybrid and dual signatures to transition to new PQ algorithms. Their aim is to help improve standards and guide the market towards an easier transition," said Wetmore.

However, Wetmore adds that "everyone is waiting on NISTs recommendations, but that is not expected until 2022-2023. Depending on the approach that's selected, all the governing bodies will need to adopt the changes and upgrade their own standards to reflect the approach."

NIST call for "hybrid" or "dual" modes

Wetmore comments that "it has been clear to the experts for some time, that there is a need to address transitions in the trusted crypto infrastructure by providing Hybrid approaches.

"Hybrid approaches are roughly described as methods which incorporate a classic crypto and a PQ crypto component into a solution. There are many challenges to implementation and trust infrastructure when attempting to hybridize.

"Hybrid modes provide protection against further cryptanalytic breakthroughs until we have confidence in PQC," said Wetmore.

Cryptographic Center of Excellence

Entrust's solution to this post-quantum security threat is the Cryptographic Center of Excellence, a group responsible for establishing an enterprise-wide strategy for crypto and PKI.

Wetmore adds: "They are the central point of contact within the organisation responsible for crypto and PKI issues - going beyond technology to provide guidance to projects and teams and help with compliancy. They take ownership for the convergence, management, and roadmap of crypto, keys, secrets and certificates."

Entrust are at the forefront of post-quantum cryptography as participating members of the IETF, and participants in the NIST PQ Competition. They have only draft for dual mode that's being looked at.

According to Gartner, organizations with crypto-agility plans in place will suffer 60% fewer cryptographically related security breaches and application failures than organisations without a plan.

"There are different approaches on how to prepare for secure cryptographical communications in a post quantum age. Using a hybrid approach is one of the more popular methods being proposed as a way of transitioning to the as yet undefined PQ algorithms. The hybrid approach suggests that rather than trust one algorithm, it places traditional algorithms like RSA and ECC alongside new PQ algorithms. This is helpful for current use cases while pre-quantum is an acceptable method for authentication and to test IT ecosystems against PQ algorithms. What we're talking about here is backward compatibility. Trying to solve the problem of starting to roll out PQ crypto before all applications are upgraded to support the new algorithms," says Wetmore.

Wetmore asserts that the Post-Quantum community (for example, surrounding the NIST PQC competition), is pushing for "hybridized" crypto that combines RSA/ECC with new primitives in order to hedge our bets against both quantum adversaries, and also algorithmic/mathematical breaks of the new primitives.

"Everybody knows RSA and ECC – they have known issues but they provide trust. By merging them, you get that classic trust but with quantum resistance of PQ algorithms. Solutions are FIPS-compliant as long as one component is FIPS-compliant; Ex {RSA + Dilithium}."

44.Tiny Magnets Could Hold The Secret to Miniaturizable Quantum Computers

by Argonne National Laboratory
https://scitechdaily.com/tiny-magnets-could-hold-the-secret-to-miniaturizable-quantum-computers/

From MRI machines to computer hard disk storage, magnetism has played a role in pivotal discoveries that reshape our society. In the new field of quantum computing, magnetic interactions could play a role in relaying quantum information.

In new research from the U.S. Department of Energy's (DOE) Argonne National Laboratory, scientists have achieved efficient quantum coupling between two distant magnetic devices, which can host a certain type of magnetic excitations called magnons. These excitations happen when an electric current generates a magnetic field. Coupling allows magnons to exchange energy and information. This kind of coupling may be useful for creating new quantum information technology devices.

"Remote coupling of magnons is the first step, or almost a prerequisite, for doing quantum work with magnetic systems," said Argonne senior scientist Valentine Novosad, an author of the study. "We show

the ability for these magnons to communicate instantly with each other at a distance."

This instant communication does not require sending a message between magnons limited by the speed of light. It is analogous to what physicists call quantum entanglement.

Following on from a **2019 study**, the researchers sought to create a system that would allow magnetic excitations to talk to one another at a distance in a superconducting circuit. This would allow the magnons to potentially form the basis of a type of quantum computer. For the basic underpinnings of a viable quantum computer, researchers need the particles to be coupled and stay coupled for a long time.

In order to achieve a strong coupling effect, researchers have built a superconducting circuit and used two small yttrium iron garnet (YIG) magnetic spheres embedded on the circuit. This material, which supports magnonic excitations, ensures efficient and low-loss coupling for the magnetic spheres.

The two spheres are both magnetically coupled to a shared superconducting resonator in the circuit, which acts like a telephone line to create strong coupling between the two spheres even when they are almost a centimeter away from each other – 30 times the distance of their diameters.

"This is a significant achievement," said Argonne materials scientist Yi Li, lead author of the study. "Similar effects can also be observed between magnons and superconducting resonators, but this time we did it between two magnon resonators without direct interaction. The coupling comes from indirect interaction between the two spheres and the shared superconducting resonator."

One additional improvement over the 2019 study involved the longer coherence of the magnons in the magnetic resonator. "If you speak in a cave, you may hear an echo," said Novosad. "The longer that echo lasts, the longer the coherence."

"Before, we definitely saw a relationship between magnons and a superconducting resonator, but in this study their coherence times are much longer because of the use of the spheres, which is why we can see evidence of separated magnons talking to each other," Li added.

According to Li, because the magnetic spins are highly concentrated in the device, the study could point to miniaturizable quantum devices. "It's possible that tiny magnets could hold the secret to new quantum computers," he said.

The magnonic devices were fabricated at Argonne's Center for Nanoscale Materials, a DOE Office of Science user facility.

A paper based on the study, "Coherent coupling of two remote magnonic resonators mediated by superconducting circuits," was published in the January 24 issue of Physical Review Letters.

45.Terra Quantum Nets $75M for Cryp-

tography, Security Work

by Brandon Vigliarolo
https://www.theregister.com/2022/04/01/terra_quantum_funding/

A Swiss quantum computing company claiming a world-first discovery has just marked what it believes is one of the largest funding rounds in the history of the quantum tech space.

Terra Quantum announced on Thursday it extended its Series A funding to $75 million, which it said will go toward strengthening its offerings in cryptography and cybersecurity.

Alongside its funding announcement, Terra also mentioned a recent breakthrough it says it had in its ferroelectricity research, which it claimed will be key to further miniaturization of electronics.

Ferroelectricity is a characteristic of some materials, such as aluminum nitride, whose electric polarization can be reversed by applying a strong enough electric field. Terra wasn't terribly forthcoming on the particulars of its breakthrough in its announcement, though said its technology can be used to build ferroelectric nanodot transistors, and has been peer reviewed.

"In the 9th issue of Nature Partner Journal: Computational materials, Terra Quantum researchers describe practical design of the ferroelectric nanodots-based negative capacitance field-effect transistor," it wrote.

We couldn't find a 9th issue of that journal online, though in the 8th issue, there's an article dated March 28, 2022, authored by a couple of Terra Quantum staff and three academics, titled: the ferroelectric field-effect transistor with negative capacitance.

If this component works, it could be a high-performance nanodot-scale transistor – transistors being a building block of modern electronics – paving the way for ever-more tiny circuits and systems.

Brain-speed ferroelectric computers?

With its discovery, Terra claimed it unlocked a key foundation for future technology, specifically terahertz-frequency-based electronics, non-invasive medical diagnostic tools, intra/inter-chip wireless interconnects for more compact equipment, 6G hardware, and more. Most of that is enabled by terahertz signals switched by tiny transistor gates.

Where Terra starts to go out on a supercomputing limb is its claims that it can build ferroelectric logical units that are apparently capable of multi-bit quantum logic, and that these will help it implement neuromorphic spiking neural networks that think like human brains. Terra believes it can use the "multi-bit logic of ferroelectric units as a model for qubits."

- IBM forges entanglement to double quantum simulations by 'cutting up a larger circuit into smaller circuits'

- Fujitsu claims 'major technical milestone' in quantum simulation
- HSBC taps IBM to explore quantum for financial applications
- Alphabet spins off quantum AI 'Sandbox'

Quantum computing is still in its infancy, with the most basic of building blocks (like a sustained qubit) still the subject of experiments and research papers instead of new hardware. Some of the most basic promises of quantum computing, like being able to break traditional encryption with ease, are also still solidly in the "maybe" category.

Despite that, investment in quantum computing has continued to rise, with some predictions seeing the industry grow 50 percent each year from now until 2027. The US government has invested considerably in quantum computing, especially securing them, and venture capital firms have been giving billions away to startups in the hope their investment in quantum computing will be the one that strikes gold.

