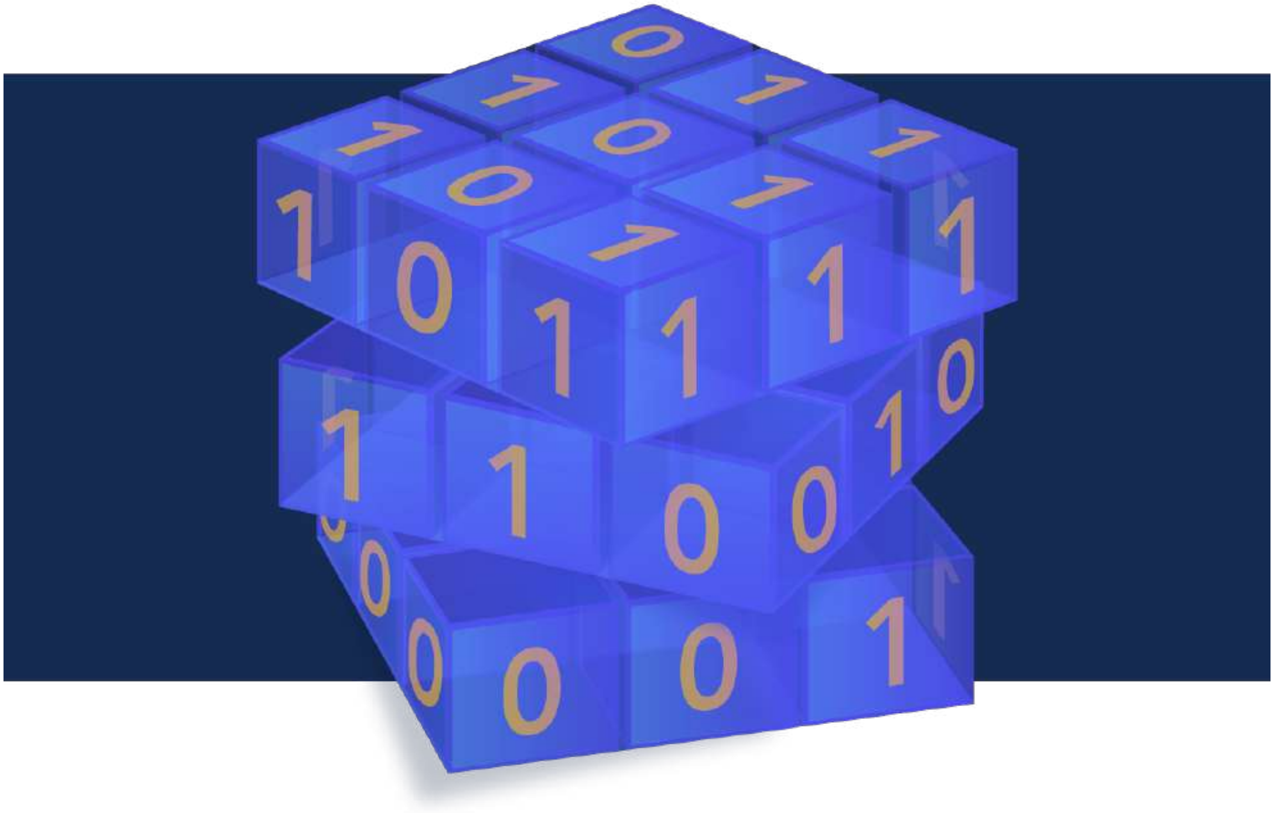
Crypto News

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

April 01, 2023



TABLES OF CONTENTS

Editorial

Happy April Readers! Let's get started with some positive news. The Canadian Defence Organization has released a roadmap to ensure that the Department of National Defence (DND) and the Canadian Armed Forced (CAF) are prepared for the "disruptive potential of quantum technologies for defence and security over the next seven years." The plan is called the Quantum Science and Technology Strategy Implementation Plan, or Quantum 2030 for short. This is yet another example of a government taking quantum technology seriously and planning for it proactively. Take a look at *article 3* to learn more about the steps the Canadian government is taking to be quantum ready.

By now we've all heard, and likely experimented with, ChatGPT. We have already seen obvious security and privacy concerns created by organizational employees looking to expedite their work by inputting sensitive information into ChatGPT. We've also already seen other AI technologies write more convincing phishing emails and ChatGPT is no different when it comes to this use of the technology. Besides these issues, there are a host of others being discussed amongst Cybersecurity professionals. However, are there any positive uses of ChatGPT and other similar technologies for the field of Cybersecurity? The author of *article 15* would like to think so. Read to find out more. Do you agree?

With most companies re-evaluating their budgets to align with the current and projected economic climate, you may find yourself trying to figure how to do more with less. Especially when it comes to Cybersecurity which most organizations consider a top priority but are choosing to cut budgets for anyway. There are some logical reasons for the cuts but the result still is that Cybersecurity leaders and their teams will need to get intelligently creative with their Cybersecurity roadmaps. Take a look at *article 25* which outlines seven levers you can pull to optimize Cybersecurity cost while still balancing your security needs. As always, enjoy this edition of Crypto News!

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

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

1.The Duality That Is Our Reality: RSA Predictions 2023

by Shashi Kiran
https://www.spiceworks.com/it-security/security-general/guest-article/rsa-conference-security-predictions/

As we head into RSA Conference 2023, it's important to understand the current duality we live in: the consumerization of the enterprise. This is an era of economic uncertainty and innovation. In this article, Shashi Kiran, chief marketing officer at Fortanix, dives into why there will be a focus on securing data at its core, through state of the art cryptographic technologies as well as in platforms that simplify the management of the entire lifecycle including for key management, certs, secrets management etc., at scale and across clouds including leveraging aspects of confidential computing.

On the one hand, we've seen a rise in data breaches and ransomware headlines, including from security companies themselves. On the other hand, we've also seen the power of ChatGPT and other such platforms capture headlines for their powerful AI. Couple these with emerging areas such as post quantum cryptography (PQC), and the future looks both interesting and frightening.

The boundaries between consumer trends and the enterprise are continuing to blur and they're also rapidly creating new attack vectors in the business landscape, particularly in an uncertain economic environment.

While the mobile phone and the tablets started to dissolve the boundaries as they came into the workforce, things have been taken up a notch with consumer applications entering the enterprise. Social media applications were the beginning, and TikTok opened new doors. At the same time, advancements in AI, machine learning, and other technologies have broken new barriers. What began as a novelty with ChatGPT has opened the doors to a myriad of possibilities that are in equal parts fascinating and frightening and certainly something that security and business leaders need to care about as top of mind.

I expect this dual paradox to impact the security space as well into the near future and beyond.

The Yin and Yang of Innovation

Technological innovation on its own can be exciting and inspiring, but AI can accelerate both the good and the bad.

First, the bad: on the one hand, we've seen a significant increase in data breaches and ransomware headlines, including from security companies themselves. According to the World Economic Forum, there were 1,774 organizational data compromisesOpens a new window in 2022, impacting more than 392 million individuals globally. And the cost of those breaches increases by an average of 20% each year, which equates to roughly 4-6% of the global gross domestic product.

On the other, we've also seen the power of ChatGPT, its successor GPT-4, and other such platforms capture headlines for their powerful AI. The prospect of these continually evolving AI-powered platforms is exciting because they could be used to amplify the good at scale and exponentially unlock the power of human innovation. It's important to remain cautiously optimistic, however; as is the case with just about any new technology, there are (and will continue to be) those who choose to use it for malicious purposes and illegal activity.

The Implications for Cybersecurity

As previously mentioned, even security companies are not immune. We've seen a number of traditional security vendors impacted by it. Architectures built around protecting infrastructure need to re-think how to protect data, applications and information.

Couple these trends with other emerging areas, such as post-quantum cryptography (PQC), and the future looks as if it is both arming the attacker and giving tools to the defender. Through it all, protecting intellectual property, personally identifiable information and sensitive data need to be paramount, not just for maintaining regulatory compliance but preserving the viability of an organization's existence. I anticipate greater interest, therefore, in securing data at its core through state-of-the-art cryptographic technologies and via platforms that simplify the management of the entire lifecycle – key management, certs, secrets management and so on – at scale and across clouds, building on the power of Confidential Computing.

The clear trend here is a movement toward a no-compromise, data-centric approach that's increasingly vital as organizations continue to transition their data and systems to the cloud. This approach decouples data security from infrastructure, ensuring that sensitive information remains secure even if an overarching network or ecosystem has been compromised.

Encryption, Regulations and the Promise of Success

Migrating to the cloud certainly has its benefits, but it could come with a host of challenges, including (but not limited to) a lack of data visibility, the storage, transmission and processing of private data, enterprise-class encryption and key management, and subpar access controls that put sensitive data at risk. While there are solutions for all of these, they need to be simple and easy to adopt and take a platform approach. Reducing complexity and sprawl is a vital aspect of enforcing security.

As SaaS becomes a key driver and multi-cloud becomes the norm, being able to confidently secure data, wherever it is, is an undertaking that regulated organizations should certainly invest their energy in. We are seeing large-scale interest in this approach from some of the largest Fortune 500 companies and government agencies, and we believe it is only the tip of the iceberg.

AI is here to stay. So are regulatory requirements. Sensitive data needs to be always protected. Let's collectively roll up our sleeves and just do it.

2.The U.S. Wants To Make Sure China Can't Catch Up On Quantum Computing

by Kevin Klyman
https://foreignpolicy.com/2023/03/31/us-china-competition-quantum-computing/

In January, the Netherlands and Japan—the leading suppliers of semiconductor production equipment—agreed in principle to implement the United States' October 2022 semiconductor export controls on China, stonewalling China's development of advanced semiconductors. While the details of the trilateral agreement remain murky, restrictions on the sale of AI chips and advanced machine tools to China will significantly impede China's drive for high-tech self-sufficiency.

But these restrictions are just the opening salvos in a series of unprecedented export controls on China planned by the Biden administration. After controls on semiconductors, the Commerce Department is moving on to the next emerging technology it worries China could weaponize: quantum computing. Export controls on quantum computing hardware, error correction software, and the provision of cloud services to Chinese entities are poised to become the next front in the U.S.-China tech war.

Quantum computing is a relatively new technology that uses the unique properties of quantum physics to build extremely powerful computers whose processing power comes from subatomic particles. Quantum computers could theoretically have much more computational power than today's "classical" computers, allowing them to tackle problems that are currently impossible, such as breaking advanced encryption. However, the field is still in its infancy and current quantum computers are error prone and lack any real applications.

Undersecretary of Commerce for Industry and Security Alan Estevez said last year that he would "put down money" on the United States enacting additional export controls related to quantum computing, artificial intelligence (AI), and biotechnology. Commerce Secretary Gina Raimondo doubled down on Estevez's bet in a speech at the Massachusetts Institute of Technology, saying that the United States would "bolster [its] system of export controls" and "take action to protect [its] advantage" over China with respect to quantum information science, semiconductors, AI, biotechnology, and clean energy technologies.

U.S. National Security Advisor Jake Sullivan laid out this policy in September 2022, arguing "computing-related technologies, biotech, and clean tech are truly force multipliers" and stating that United States would impose export controls in order to "maintain as large of a lead as possible" ahead of rivals such as China. In other words, because technologies like quantum computing have the capacity to provide China with military and economic advantages, whether through new cyberweapons or faster drug discovery, the United States plans to enact sweeping unilateral export controls on China.

Policymakers in Washington are determined to maintain the United States' lead in quantum computing because of its potential military applications. Researchers have warned that a potent quantum computer could thwart existing encryption schemes, leading U.S. President Joe Biden to issue a national security memorandum requiring federal agencies to shift to post-quantum cryptography by 2035.

In 2021, three Chinese quantum computing organizations were placed on the Commerce Department's Entity List, preventing U.S. firms from selling products to them without a license. The Commerce Department claimed that these Chinese quantum computing groups "support the military modernization of the People's Liberation Army" and use U.S. technologies to develop "counter-stealth and counter-submarine applications, and the ability to break encryption." But stronger measures are likely to come.

The United States and China are the two most advanced countries in quantum computing, but the United States is the clear global leader. It is ahead in three of the four most promising technical approaches to quantum computing, while China leads in just one approach. From 2011 to 2020, the United States produced the most quantum computing publications as well as twice as many highly-cited quantum computing publications as China. Additionally, U.S. quantum computing firms have 30 times more funding than private Chinese competitors – although plenty of money is going into government-backed research in China too.

While China leads the world in quantum communications, a subfield of quantum information science with the potential to enable ultra-secure data transfers, Chinese scientists acknowledge America's edge in quantum computing. Top Chinese quantum computing researcher Lu Chao-Yang recently concluded "Google's in the lead," adding that he had "no idea" how the rumor began that China had spent $15 billion on quantum computing since "the actual money is maybe 25 percent of that."

3.Canadian Defence Organizations Release Overview Of Quantum 2030

by Matt Swayne
https://thequantuminsider.com/2023/03/28/canadian-defence-organizations-release-overview-of-quantum-2030/

The Department of National Defence and Canadian Armed Forces (DND/CAF) Quantum Science and Technology Strategy Implementation Plan, known as Quantum 2030, is a roadmap to ensuring DND/CAF is better prepared for the disruptive potential of quantum technologies for defence and security over the next seven years.

Examples of the military potential of quantum technologies include positioning, navigation and timing where Global Positioning Systems (GPS) don't work; sensors to detect chemical, biological, radiological, and nuclear (CBRN) threats; secure communication and code-breaking; and advanced materials and medical research.

Research and development into emerging technologies and countermeasures will ensure DND/CAF is prepared to be an early adopter, work with allies and stay ahead of potential adversaries.

The implementation plan includes five calls to action for DND/CAF:

- Identify who is expected to use quantum technologies within DND/CAF;
- Train personnel for a base level of understanding of quantum, known as quantum literacy;
- Harmonize quantum investments across DND/CAF;
- Access state-of-the-art technology through innovation programs; and,
- Engage industry and academia.

"Quantum mechanics is the physics of the very small. The field seeks to predict and explain the behaviour of atoms and molecules and involves the manipulation and control of systems at the atomic and subatomic levels." — National Quantum Strategy

Quantum 2030 identifies four promising quantum technologies with defence and security applications and lays out a seven-year plan to develop prototypes ready to be tested in the field by the year 2030.

1. Quantum-enhanced radar
2. Quantum-enhanced light detection and ranging (LiDAR)
3. Quantum algorithms for defence and security
4. Quantum networking

The seven-year plan is divided into three phases including recruiting and training personnel, scientific development, and field testing and demonstrations.

Quantum 2030 builds on the DND/CAF Quantum Science and Technology Strategy, which was published in January 2021, and aligns with the Government of Canada's National Quantum Strategy, released in January 2023.

4.China Delivers Self-Developed Quantum Computer Core Device To Users

by CGTN
https://news.cgtn.com/news/2023-03-28/China-delivers-self-developed-quantum-computer-core-device-to-users-1ixkvKignoQ/index.html

A Chinese company successfully delivered a self-developed quantum computer core device of impedance-matched quantum parametric amplifier (IMPA) to its users, marking a new level of China's R&D and industrialization in the quantum computing field.

Jia Zhilong, deputy director of the Anhui Quantum Computing Engineering Research Center announced the delivery on Monday.

As the first-stage amplifier for quantum chip signal, the IMPA can effectively improve signal reading fidelity and signal-to-noise ratio, and it has become one of the indispensable core devices to develop practical quantum computers, said Jia.

The Chinese company, Origin Quantum Computing Technology Co, is a quantum computing company based in east China's Anhui Province.

Core device of quantum computer

According to Jia, the IMPA's equivalent noise temperature is close to the quantum limit noise level.

However, the equivalent noise temperature of conventional amplifiers far exceeds that noise level, and the effective signal is usually submerged by noise, so they can only be used for post-stage amplification of quantum links.

In the process of developing a practical quantum computer, the reading fidelity and signal-to-noise ratio of quantum chips are important indexes to measure the performance of qubits.

With a relatively high fidelity of reading and controlling of a quantum chip, quantum error correction can be performed to further improve the control precision of the quantum computer.

Self-developed device, promising applications

Developed independently by Origin Quantum, the IMPA is designed in a highly integrated manner, which can work at extremely low temperatures of 10mK-200mK.

It also has very low power consumption and is easy to be embed into large-scale application systems.

Concerning its applications, Jia said the IMPA can be used not only in the field of quantum computing, but also in fields such as precision measurement.

"We expect the delivery to play a more important role in future engineering applications in the field of science and technology.”

China's latest quantum computer Wukong will feature a chip with over 64 qubits, Zhang Hui, manager of

Origin Quantum, told guancha.cn in an interview, comparing to IBM's Osprey quantum processor with 433 qubits and Google's quantum chip Bristlecone with 72 qubits.

Zhang said the company lags behind the world's leading quantum computing players like IBM and Google in terms of hardware products and development, but has some advantages in the software and operating systems, and views the former as the way forward.

5.Qusecure And Accenture Team In First Successful Multi-Orbit Communications Link Showcasing Post-Quantum Crypto Modernization

by Dan Spalding

https://www.businesswire.com/news/home/20230328005469/en/QuSecure-and-Accenture-Team-in-First-Successful-Multi-Orbit-Communications-Link-Showcasing-Post-Quantum-Crypto-Modernization

QuSecure™, Inc., a leader in post-quantum cybersecurity, today announced that the company, in collaboration with Accenture, has accomplished the first successful multi-orbit data communications test secured with post-quantum cryptography (PQC), which refers to cryptographic methods that are secure against an attack by a quantum computer. This demonstrates that crypto-agility, successfully rotating to a less vulnerable algorithm, is real and possible.

Before this achievement, data from multi-orbit satellites could be collected and potentially broken by classical means and quantum computers with enough power. Recognizing the world's growing reliance on satellite communications, QuSecure and Accenture teamed to deliver a crypto-agile quantum-resilient channel from earth to a low earth orbit (LEO) satellite. From there, the breakthrough transmission included a switch over from LEO to a geosynchronous orbit (GEO) satellite and back down to earth, as a model for redundancy in the event of a breach, failure or threat to satellites in a single orbit.

This outcome was accomplished through an Accenture-facilitated LEO data transmission. The entire transmission was secured using both classical cybersecurity and quantum-resilient cybersecurity utilizing QuSecure's QuProtectTM platform, all with no installation of software on the satellites. This demonstrates QuProtect's ability to upgrade secure communications on existing hardware with a software layer. QuSecure's software solution is an opening salvo in the $20 billion-a-year crypto modernization effort that government and private enterprise are undertaking to implement a zero-trust architecture before quantum computers begin decrypting today's data.

“Outer space is getting more crowded and contested every day, and providing reliable space-based security is critical in today's global economy,” said Tom Patterson, Quantum and Space Security lead at Accenture. “Blue sky thinking addressing real world issues is what Accenture's clients require, and security is a critical component of delivering the best solutions around the world. Bringing advanced security capabilities like QuSecure's quantum-resistant crypto agility systems to orbit drives Accenture forward to better secure businesses on earth and throughout the space ecosystem.”

Now QuSecure and Accenture can help organizations conduct live, more secure (from both a classical and quantum security perspective) communications and data transmissions through multiple orbits in space. The flexibility, speed and abundance of LEO satellite communications (350-2,000 km altitude) can be protected by QuSecure's Quantum Secure Layer (QSL) within traditional public key infrastructure.

"As more organizations are increasingly relying on space technology to provide solutions, resiliency and more relevant information, security of those systems and the data is paramount," said Paul Thomas, Space Innovation Lead, Technology Innovation at Accenture. "Accenture's Space Innovation and Security teams are working together to ensure our partners and clients are prepared and secure as they embark on their space journeys. We are pleased to work with QuSecure in bringing crypto security to secure space data transmission."

QuSecure's same protective encryption can transmit up to GEO satellites whose 37,000 km orbit can carry more traffic with greater coverage. This enables servers, edge, IoT, battlefield, point-of-sale, and other devices outside conventional data networks to adopt quantum-safe communications using satellite communications. From secure military communications to financial payment and data transmissions, organizations now can be better protected from malicious data harvesting. Data harvested today can be decrypted by a quantum computer in the future, an active and ongoing practice known as Steal Now Decrypt Later (SNDL).

"We are thrilled to announce our work with Accenture as we embark on a revolutionary journey to secure the digital landscape through multi-orbit networking, crypto-agility, and a strong, synergistic collaboration," said Dr. Garrison Buss, QuSecure's Chief Strategy Officer. "As pioneers in post-quantum cybersecurity, our collaboration will elevate our clients' protection by leveraging the power of advanced networking solutions that span terrestrial, aerial, and space domains. Our unwavering commitment to excellence, combined with Accenture's extensive domain expertise, will drive us to deliver unparalleled security solutions in a world that is increasingly interconnected and reliant on data."

6.Vincent Rijmen Wins The Levchin Prize For Real-World Cryptography 2023

by Dana Brouckmans
https://www.esat.kuleuven.be/cosic/news/vincent-rijmen-wins-the-levchin-prize-for-real-world-cryptography-2023/

Belgian Professor Vincent Rijmen wins the Levchin Prize for Real-World Cryptography 2023

The Levchin prize honors major innovations in cryptography that have had a significant impact on the practice of cryptography and its use in real-world systems. The Belgian Prof. Vincent Rijmen received on Monday March 27th the 2023 Levchin prize for his many contributions to the field. He is known in the first place as designer of Rijndael, which was elected as the Advanced Encryption Standard (AES) in 2000. Nowadays AES is used worldwide to secure the Internet, WiFi, communication via cell phones, smartcards, payments, etc. This is the reason why all modern PC processors include special circuitry to accelerate AES.

Prof. Rijmen was involved in several other cryptographic developments that are relevant in real-world systems. He contributed to a mechanism used by the Galileo satellites to secure their navigation signals against hackers and foreign services. He invented the Threshold Implementation (TI) method that is used by large manufacturers like NXP to secure their smartcards.

An important contribution at academic level is the book on Rijndael that he wrote with his colleague. Thousands of researchers and developers all over the world to learn from this book the principles of modern cryptographic design.

Prof. Rijmen accepts this award as an encouragement to continue his work on the development of a real-cryptography world, where citizens can rest assured that they are in control of their data and that their "smart" devices are protected against criminal hackers.
Vincent Rijmen is full professor with KU Leuven, Belgium and adjunct professor with University of Bergen, Norway.

7.India's First Quantum Computing-Based Telecom Network Link Now Operational

by PTI
https://economictimes.indiatimes.com/tech/technology/indias-first-quantum-computing-based-telecom-network-link-now-operational-ashwini-vaishnaw/articleshow/99039710.cms

IT and telecom minister Ashwini Vaishnaw on Monday said the country's first quantum computing-based telecom network link is now operational in the national capital.

While speaking at the first international quantum enclave, Vaishnaw said the quantum communication link is now operational between Sanchar Bhawan and National Informatics Centre office located in CGO Complex in the national capital.

"The first quantum secure communication link between Sanchar Bhawan and NIC, CGO complex is now operational," Vaishnaw said and announced a Rs 10 lakh prize money for ethical hackers who can break the encryption of the system.

"We are also launching a hackathon, a challenge round, for anybody who breaks this system and system developed by C-DoT, we will be giving Rs 10 lakh per break," Vaishnaw said.

The minister inaugurated a small exhibition of quantum computing firms and invited them to run pilot projects for communications networks and Indian Railways.

Conversation AI chatbot soon?

Vaishnaw on Monday hinted at a "big announcement" in a few weeks regarding conversational AI tools. To a specific question on whether India can build something equivalent to the conversational AI tool ChatGPT, the minister said "wait for a few weeks, there will be a big announcement".

When asked about what the big announcement might will be, the minister declined to give further details and said, "Parliament is in session, so I cannot say anything…"

Vaishnaw was speaking at the India Global Forum event.

It is pertinent to mention that ChatGPT has dazzled the world with its conversational skills and triggered an AI (Artificial Intelligence) chatbot race.

The new AI chatbot tool - created by the San Francisco artificial intelligence company OpenAI - has over the past weeks exploded in popularity and grabbed headlines.

It can be tasked to provide definitive answers to questions, responds to user prompts, and based on online information, it can churn out scripts, speeches, song lyrics, homework material, articles, marketing copy, classroom essays and even draft research paper abstracts.

8.First Quantum Computer Made In Japan By Riken Put Online

by Mutsumi Mitobe
https://www.asahi.com/ajw/articles/14871014

Japan's first domestically produced quantum computer, developed by the Riken research institute, was released online on March 27 to allow joint researchers to access it.

"The release is not a goal, but a milestone," said Yasunobu Nakamura, director of the Riken Center for Quantum Computing in Wako, Saitama Prefecture, who led the development of the domestically produced computer.

"The race has just begun," he added.

There are many challenges to overcome before putting the quantum computer, considered to be the next generation of computers, into practical use, but it has the potential to change society.

The international competition to develop quantum computers is intensifying in the hopes of gaining an economic advantage and stronger national security.

Japan aims to accelerate developing related industries and human resources in the country with a focus on a domestically produced computer.

Unlike conventional computers, quantum computers use quantum mechanics, an area of physics that describes the behaviors of micro particles such as electrons and atoms, to perform calculations.

As a quantum computer can perform multiple calculations at once, it can sometimes easily solve problems that a supercomputer cannot solve even if it spends tens of thousands of years or hundreds of millions of years.

Quantum computers are expected to advance research in fields that require complex calculations, such as developing new materials and medicine, finance and artificial intelligence.

A quantum computer will also make it easier to decipher current encryptions used on the internet and in finances.

As the technology develops, there is concern that a quantum computer could be used to decode national security secrets as well. Countries such as the United States and China regard this as a security issue and are heavily investing in developing the technology.

There are various ways to create quantum computers, but Japan's domestic computer uses the superconducting method. The quantum bit, the core component of a quantum computer, is made of superconducting materials and cooled to extremely low temperatures.

Google and International Business Machines Corp. are also working on developing computers using the same method.

The Japanese government aims to achieve a quantum computer that can be widely used in practical applications in 2040 and after, but it is said that about 1 million quantum bits would be needed to create it.

The current domestic quantum computer has 64 quantum bits.

Only dozens to hundreds of quantum bits are used in quantum computers that have so far been created in the world, making practical use a long way off.

Some predictions suggest that a quantum computer could produce values of more than 100 trillion yen ($765 billion) within 15 to 30 years.

With its domestically produced quantum computer, Japan stands at the starting point of the development race.

9.What Are The Remaining Challenges For Quantum Computing?

by Matt Swayne
https://thequantuminsider.com/2023/03/24/what-are-the-remaining-challenges-for-quantum-computing/

By any measure, the progress on developing quantum computers for practical purposes — even over the last few years — has been nothing less than stunning. Still, quantum scientists and engineers are just at the foothills on their climb to the summit of scalable, general quantum computing. In this article, we'll look at the main challenges that these researchers must solve before we can use quantum computers for more everyday problems, such as finding treatments for diseases and medical conditions and discovering new materials for a sustainable economy.

WHAT MAKES QUANTUM COMPUTING SO DIFFICULT?

Quantum computing uses quantum bits, or qubits, instead of classical bits. Qubits have weird properties, at least when compared to our classical computing reality. Qubits can exist in a superposition of states, meaning they can represent multiple values at the same time, and they can also become entangled with each other, allowing for parallel computation. This makes quantum computing potentially much faster than classical computing for certain types of problems, such as factorization and database searching.

However, quantum computing is also challenging for several reasons. The biggest challenge, arguably, is qubit decoherence. Qubits are extremely sensitive to their environment, and even small disturbances can cause them to lose their quantum properties, a phenomenon known as decoherence. The struggle to master decoherence may require new materials, new computational techniques and deep exploration of various quantum approaches. It's not just hardware. Quantum algorithms are much more complex than classical algorithms and require developers to approach computational problems in original ways.

WHAT ARE REMAINING CHALLENGES?

This complexity has created the following challenges for quantum computing scientists, engineers and entrepreneurs.

Error Correction

Most experts would consider this the biggest challenge. Quantum computers are extremely sensitive to noise and errors caused by interactions with their environment. This can cause errors to accumulate and degrade the quality of computation. Developing reliable error correction techniques is therefore essential for building practical quantum computers.

Scalability

While quantum computers have shown impressive performance for some tasks, they are still relatively small compared to classical computers. Scaling up quantum computers to hundreds or thousands of qubits while maintaining high levels of coherence and low error rates remains a major challenge.

Hardware Development

Developing high-quality quantum hardware, such as qubits and control electronics, is a major challenge. There are many different qubit technologies, each with its own strengths and weaknesses, and developing a scalable, fault-tolerant qubit technology is a major focus of research.

Software Development

Quantum algorithms and software development tools are still in their infancy, and there is a need for new programming languages, compilers, and optimization tools that can effectively utilize the power of quantum computers.

Classical Computers Interfaces

Quantum computers won't replace classical computers; they will serve as complementary technology. Developing efficient and reliable methods for transferring data between classical and quantum computers is essential for practical applications.

Standards and Protocols

As the field of quantum computing matures, there is a need for standards and protocols for hardware, software, and communication interfaces. Developing these standards will be essential for ensuring compatibility and interoperability between different quantum computing platforms. We should also throw in benchmarking — the ability to measure performance standards is still in its infancy for quantum computing design, development and operation.

Trained Talent

The number of people properly educated and trained to enter the quantum workforce is small and spread across the world. Finding the right workers is a challenge. In a chicken-and-egg scenario, we won't increase the number of people motivated to enter the quantum workforce until we have more practical quantum computers and we won't have more practical quantum computers until we have more people motivated to become part of the quantum workforce.

Overall Expense

Perhaps this is an obvious outcome of all the above challenges, but expense remains a huge roadblock — or stumbling block — for quantum computing. The likelihood that two Steves will be slapping together quantum computers in their garage is an unlikely scenario. Quantum talent is expensive. Quantum hardware is expensive. Supply chains are complex, vulnerable and — you guessed it — expensive to establish and maintain. Dealing with these expenses and finding investments to offset these costs will likely be a standard duty of institutional scientists and commercial entrepreneurs for the foreseeable future.

CHALLENGING IS NOT IMPOSSIBLE

The list is a little daunting, but there are lots of reasons for hope. Funding agencies, such as government agencies, are rising to the occasion to invest in tackling these quantum challenges. Researchers — almost daily — are making advances in the engineering and scientific challenges to create practical quantum computers.

Finally, it might not be one giant leap that lands humankind on the summit of Mount Quantum. Rather, it will take many small advances, many tiny legislative victories and lots of little commercial wins that will surmount these challenges.

10.IBM And Fundación Ikerbasque Partner To Launch Groundbreaking Quantum Computational Center

by Miguel Gimenez de Castro and Chris Nay
https://newsroom.ibm.com/2023-03-24-IBM-and-Fundacion-Ikerbasque-partner-to-launch-groundbreaking-Quantum-Computational-Center

Fundación Ikerbasque, the Basque Foundation for Science in the Basque Country of Spain, and IBM today presented details of how they are partnering to further establish the Basque Country as a leading technology hub. This includes the adoption of quantum computing through the launch of the IBM-Euskadi Quantum Computational Center, which will provide Qiskit Runtime services from a 127-qubit IBM Quantum System One located in San Sebastian and managed by IBM.

IBM and IkerBasque share a common mission on the role of quantum computing as a key element of the Basque Country Government's Ikur 2030 vision for quantum technologies. This initiative aims to advance quantum research, build a quantum workforce, promote economic development, and provide the necessary quantum computing infrastructure to achieve those goals. The IBM-Euskadi Quantum Computational Center will promote the use of advanced technology across all the Basque Country Government and the General Deputations (Araba, Bizkaia and Gipuzkoa), further elevating research institutions by expanding international research collaborations, performing world-class fundamental scientific research, and increasing the quantum-trained talent in the region.

To achieve these goals, the new IBM-Euskadi Quantum Computational Center will focus on collaborations in crucial areas such as materials research, to develop a world-class, leading quantum ecosystem in Southern Europe that will leverage the strengths of its provinces to drive the advancement of science and technology.

This IBM-Euskadi Quantum Computational Center will provide computational infrastructure for researchers from Ikerbasque Foundation and its partners to help researchers meet these goals. Researchers will be able to run quantum programs to explore complex problems, including the modeling of new materials and how quantum computing can be used as part of broader sustainability efforts. The IBM Qiskit Runtime services made available via this collaboration will leverage an IBM Quantum System One to be deployed at the Ikerbasque building located in San Sebastian (Guipuzkoa - Spain). This new center represents a further step in promoting technology development in the region to expand the horizons of computation.

IBM and Ikerbasque will also collaborate to develop workforce programs aimed at building and establishing world-class talent in the Basque Country. The IBM-Euskadi Quantum Computational Center programs will drive internal and external awareness, education, and skill building through the development of immersive and integrated learning programs.

“It is very risky to say what the future of quantum computers will bring us. Nobody knows for sure. What we do know for sure is that the Basque Country must be prepared for the future. It is essential to be in a good starting position for when the situation requires it. Euskadi joins today, a select group of IBM Quantum Computational Centers. We will actively collaborate with this Network and we will contribute all our knowledge to continue developing this technology. IBM’s commitment to the Basque Country reflects a new recognition of our science, technology and innovation system. The Basque Country believes in science and invests in it. We do so, convinced that our welfare will come through progress, through scientific advances,” assured the President of the Basque Country Government, Mr. Iñigo Urkullu.

“The IBM-Euskadi Quantum Computational Center is further proof of our commitment in building open communities of innovation to tackle the most challenging problems of our time,” said Dr. Darío Gil, Senior Vice President and Director of Research, IBM. “This partnership will bring to bear the full scope of IBM's quantum technologies to The Basque Country’s world-class scientific and industrial communities. We are proud to be working with the Government of The Basque Country, as well as private sector and academic partners, to take innovation in Spain to the next level.”

The IBM-Euskadi Quantum Computational Center is the second such IBM Quantum Computational Center to be announced in Europe. Ikerbasque will join the more than 200 members of the IBM Quantum Network, a global community of Fortune 500 companies, start-ups, academic institutions, and research labs working to advance quantum computing and explore practical applications. These leading institutions have access to IBM’s Quantum-as-a-Service computing resources. Since 2016, IBM has deployed over 60 quantum computers for external use. There are now more than 20 quantum computing systems, including the 433-qubit IBM Osprey processor.

11.The Quantum Insider Report Details China’s Emergence As A Global Leader In Quantum Investment And Research

by Matt Swayne
https://thequantuminsider.com/2023/03/23/the-quantum-insider-report-details-chinas-emergence-as-a-

global-leader-in-quantum-investment-and-research/

China appears poised to be the leader in the global quantum market, according to a report from The Quantum Insider (TQI), the leading provider of news and market intelligence on the quantum technology industry. The report provides in-depth coverage of historical investment trends, regulatory developments, key Chinese quantum companies and investors.

Growing tensions between China and the US over the past decade have fueled China's race to achieve technological independence, resulting in significant public and private investment in high-tech sectors, including quantum computing. The report highlights the importance of quantum and its varied applications, particularly in the areas of security and defense, which have rendered it one of the key areas of interest for China.

The report details that China is considered the global leader in quantum communications, with recent breakthroughs such as the world's first successful launch of a quantum-enabled satellite and the establishment of a 4,600+ km quantum communications network. Additionally, China's ongoing education modernization initiatives, including special quantum programs, will tackle any resourcing and talent issues in the future.

China is estimated to have committed significant government funding in quantum. Although actual funding levels are difficult to accurately calculate, the report notes confirmed funding is at least $4 billion with many sources guiding to funding of over $17 billion. The upper end of the range would amount to approximately double the total committed funding across the EU (or 4x the US). The exact budget breakdown for the amount is not public but is understood to include a significant construction component for the world's largest quantum research facility, the 37-hectare National Laboratory for Quantum Science in Hefei.

"As a leading market intelligence company, we are committed to providing our clients with the most comprehensive and up-to-date information on emerging trends in quantum computing," said Alex Challans, CEO of Resonance, the holding company that owns TQI. "Our latest report on China's emergence as a global leader in quantum investment and research is something many of our clients have been asking for and we're excited to finally share our work."

The report highlights that close public-private cooperation in the Chinese quantum market, and significant government involvement, even in the 'private' sphere, are driving the country's advancements. Private investment into quantum in China reached $255 million in 2022, significantly below international VC activity, though real investment levels are likely higher.

The report will be available for free to premium subscribers to TQI's intelligence platform and is available to preview and purchase standalone in the quantum reports section.

12.Indian Startup BosonQ Psi Joins IBM's Quantum Computing Program

by Team TC
https://www.techcircle.in/2023/03/23/indian-startup-bosonq-psi-joins-ibm-s-quantum-computing-program

Bengaluru-based BosonQ Psi, a Quantum SaaS software startup, has joined IBM's Quantum Network startup program to develop quantum algorithms for simulations on quantum systems. Through the program, the startup will gain access to IBM's Qiskit libraries, simulators, and quantum systems available over the cloud.

Founded in 2020, BosonQ Psi's core service is BQPhy, a quantum-powered engineering simulation software, which uses quantum computers to perform complex simulations in much lesser time than traditional software running on a regular PC or supercomputer. The alpha version of BQPhy is available to customers via the cloud. Its full-scale version is expected to be released in mid-2023.

"We are getting overwhelming traction for our simulation platform. Being part of IBM's network allows our team to experiment and harness the scalability of our hybrid quantum-classical algorithms and carry out proof-of-concept projects," said Rut Lineswala, founder and chief technology officer of BosonQ Psi.

IBM is one of the few companies in the world that opens a quantum computer and has developed several solutions that have made the quantum application possible. A case in point is Qiskit Runtime, which is a containerised runtime software that runs on IBM Cloud and uses classical computers to optimise workloads and then efficiently executes them on quantum systems.

The US company is also working on a quantum computer with a modular architecture powered by a 4,000 qubit processor. Similar to its startup program, IBM has a Quantum Network for enterprises, which includes Bosch, Vodafone, and French bank Credit Mutuel Alliance Federale. These companies are working with IBM to explore use cases for quantum computing in their sectors.

"India's quantum ecosystem growth is vitally important to the quantum industry. We believe that BosonQ Psi's membership in the IBM Quantum Network will broaden the opportunity for this community of domain experts to learn and explore how quantum computing can help their organizations," said Aparna Prabhakar, vice president of IBM Quantum Ecosystem.

Though quantum computing is still in its early stages, India has shown a lot of interest to leverage their computing power. In addition to announcing ₹8,000 crore National Mission on quantum computing in the 2020 budget, the Indian government also launched a quantum simulator called QSim in August 2021. It allows researchers to simulate quantum computation on classical supercomputers through a web browser.

Several IT firms in India are planning to tap into it to offer quantum as a service to their enterprise customers in the near future.

Quantum computers use principles of quantum physics to process information simultaneously and use an alternative form of computing, which allows them to run complex computations that are beyond the capacity of traditional computers including supercomputers.

13.The Top 10 Benefits Of Using An HSM For Data Security

by Newsmantraa

https://www.digitaljournal.com/pr/news/the-top-10-benefits-of-using-an-hsm-for-data-security

In today's digital age, data security has become an essential aspect of modern-day business operations. With the rise in cyberattacks and data breaches, organizations need to adopt robust security measures to safeguard their sensitive information.

One of the most effective ways to do this is by using a Hardware Security Module (HSM). In this article, we'll explore the **top 10 benefits of using an HSM for data security**.

Benefit 1: Stronger Encryption

Encryption is the process of converting plaintext into ciphertext to prevent unauthorized access to sensitive data. The stronger the encryption, the harder it is for hackers to gain access to data. HSMs provide a secure environment for key generation and storage, ensuring that the encryption keys are not accessible to unauthorized parties.

With HSMs, organizations can leverage advanced encryption algorithms, such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), to enhance the security of their sensitive information.

Benefit 2: Protection Against Data Breaches

A **data breach** occurs when unauthorized individuals gain access to confidential data. Data breaches can be costly, both financially and in terms of reputational damage. HSMs offer protection against data breaches by encrypting sensitive data and ensuring that only authorized individuals have access to the encryption keys.

In the event of a breach, HSMs can also help in limiting the damage by allowing for remote destruction of the encryption keys.

Benefit 3: Compliance with Security Regulations

Many organizations are required to comply with **security regulations** when HSM is at the stake. These regulations are some of the commonly recognized compliance standards for HSMs.

The PCI DSS is a set of security standards that applies to organizations that handle credit card data. The standard requires the use of HSMs to protect cardholder data and cryptographic keys. In addition to this, Federal Information Processing Standards (FIPS) 140-2/3 is a U.S. government standard that specifies security requirements for cryptographic modules. The standard requires the use of HSMs for cryptographic modules used in federal government systems.

General Data Protection Regulation (GDPR) is a European Union regulation that sets standards for data protection and privacy. The regulation recommends the use of HSMs to protect personal data and cryptographic keys.

While choosing an HSM, it is recommended to check its own certifications, also. Common Criteria, EAL4+, RoHS, PCI PTS HSM 3.0 / 4.0 certifications are essential certifications for HSM devices.

Common Criteria is an international standard for IT security evaluation, validation, certification of security products and EAL, which stands for The Evaluation Assurance Level (EAL), is a numerical rating assigned to IT products to indicate the depth and rigor of their security evaluation. EAL4+ is the highest EAL level that a commercial product can achieve, and it indicates that the product has undergone extensive testing and evaluation to ensure that it meets strict security requirements.

Another important certification for an HSM device is RoHS, The Restriction of Hazardous Substances (RoHS) Directive, is a European Union directive that restricts the use of certain hazardous substances in electronic and electrical equipment. HSM devices that comply with RoHS do not contain lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls (PBBs), or polybrominated diphenyl ethers (PBDEs).

Lastly, PCI PTS HSM, The Payment Card Industry (PCI) PIN Transaction Security (PTS) HSM certification is a security standard developed by the PCI Security Standards Council for HSMs used in the processing of cardholder data. It sets specific requirements for the design and testing of HSMs to ensure the confidentiality and integrity of sensitive data.

HSMs can help organizations comply with these regulations by providing secure key management and encryption processes that meet the specific requirements of each regulation. Each of these certifications provides additional assurance that an HSM device meets specific security and safety requirements. It is important to determine which certifications are relevant for your specific use case and select an HSM device that has the appropriate certifications.

Benefit 4: User Authentication

User authentication is the process of verifying the identity of individuals accessing a system or network. HSMs can aid in user authentication by providing secure key storage and management for authentication keys.

With HSMs, organizations can ensure that only authorized users have access to sensitive information and that their identities are authenticated before they are granted access.

Benefit 5: Key Management

Key management is the process of generating, storing, distributing, and revoking encryption keys. Effective key management is crucial to ensuring the security of sensitive data. HSMs offer secure key management by providing a dedicated hardware device that stores and protects encryption keys.

This ensures that only authorized individuals have access to the keys and that they are not vulnerable to attack or theft.

Benefit 6: Improved Performance

The use of HSMs can improve the performance of cryptographic operations such as encryption and decryption.

HSMs offload the processing of cryptographic operations from the server or workstation to a dedicated hardware device. This can result in faster cryptographic operations and **improved system performance**.

Benefit 7: Cost Savings

HSMs can offer **cost savings** by reducing the need for expensive hardware upgrades and the cost of maintaining a secure key management system. HSMs provide a secure hardware environment for key generation and storage, eliminating the need for expensive key management software and hardware.

This can result in significant cost savings for organizations that require secure key management.

Benefit 8: Flexibility

HSMs offer flexibility in terms of the types of cryptographic operations they can perform and the platforms they support. HSMs can be used to perform a wide range of cryptographic operations, including encryption, decryption, digital signature, and key management.

They can also be used with a variety of platforms, including servers, workstations, and mobile devices.

Benefit 9: Disaster Recovery

HSMs can aid in **disaster recovery** by providing a secure backup of encryption keys. In the event of a disaster or system failure, organizations can use the backup keys to recover their encrypted data. This ensures that sensitive data is not lost or compromised in the event of a disaster.

Benefit 10: Scalability

HSMs offer scalability in terms of the number of users and applications they can support. HSMs can support multiple users and applications, allowing organizations to scale their security infrastructure as needed. This can be particularly beneficial for organizations that are experiencing rapid growth or that need to accommodate a large number of users or applications.

In conclusion, **Hardware Security Modules** (HSMs) offer a range of benefits for organizations seeking to enhance their data security. From stronger encryption to disaster recovery, HSMs provide a secure hardware environment for key generation and storage, ensuring that sensitive information remains confidential and protected. With the rise in cyberattacks and data breaches, HSMs are becoming an essential tool for modern-day business operations.

14.How To Prepare Your Business For The Post-Quantum Cryptography Transition

by Alice Cumming
https://www.businessleader.co.uk/how-prepare-your-business-post-quantum-cryptography-transition/

In this guest article, Dr Ali El Kaafarani, CEO of PQShield, a cybersecurity company specialising in post-quantum cryptography, discusses how businesses can begin the migration to post-quantum cryptography and prepare for a quantum-secure future.

Quantum computing is an emerging technology that has the potential to revolutionise industries from finance to healthcare. In 2021, $31bn of public funding into quantum technologies was announced by governments across the world, while $4.1bn (£3.3bn) was raised by quantum start-ups.

The ecosystem for quantum innovation is flourishing – there are now over 212 startups dedicated to developing quantum technologies. Meanwhile, the UK government has launched its long-awaited National Quantum Strategy creating a new 'Office for Quantum' in the Department for Science, Innovation and Technology (DSIT) and committing £2.5bn in funding for the sector over the next ten years.

But quantum computers also have the potential to completely undermine businesses' cybersecurity by rendering current cryptographic methods useless. Late last year, the Secretary General of the UN offered a stern and timely warning: "Quantum computing could destroy cybersecurity."

The quantum threat

Quantum computers pose a cybersecurity threat because they can perform certain types of calculations much faster than classical computers. Specifically, they can efficiently solve problems that are considered to be intractable for classical computers, such as factoring large numbers.

Unfortunately, these mathematical problems underpin much of the cryptography that's relied on today to protect sensitive information, putting it at risk of easy decryption by a quantum computer.

There has been a lot of focus on new cryptographic schemes and algorithms to combat the quantum threat, but there is also a knock-on effect to the methods by which these are securely implemented – for example the techniques for guarding against side-channel attacks also have to be significantly evolved, tested and validated before critical devices can be considered fully secure.

In short, the security paradigm has shifted. Businesses can no longer code and forget or assume that hardware will be protected forever. The quantum threat means that all software and hardware is at risk of being compromised by quantum computers, possibly within the next decade.

Building quantum defences

In July last year, the US National Institute of Standards and Technology announced a major milestone in its efforts to standardise post-quantum cryptography, a new type of encryption that can withstand even powerful quantum computers. With these draft standards published, companies now have the guidance they need to start putting quantum defences in place.

Given that quantum computers are not yet commercially viable, it is easy for business leaders to think that they can kick the can down the road and delay the migration to post-quantum cryptography.

But this is a serious mistake – the quantum threat is all the more urgent because of the looming threat of 'harvest now, decrypt later' attacks, by which adversaries can gather sensitive data today to decrypt as soon as they have their hands on a sufficiently powerful quantum computer. In a recent survey by Deloitte of over 400 cybersecurity professionals, half (50.2%) of respondents believe their organisations are at risk from such attacks.

There are definitely some sectors which are leading others in terms of preparedness and laying down plans to thrive in a post-quantum world. Some businesses in highly regulated industries, such as finance, defence or healthcare, have already begun the migration to post-quantum cryptography.

Last year, for example, Mastercard announced that it has started incorporating post-quantum cryptography into its contactless cards. More broadly, nearly a third of businesses are already at the strategic planning stage preparing for the quantum threat and the commercialisation of quantum technologies.

Preparing your business for post-quantum cryptography

There are many who recognise the seriousness of the quantum threat but don't actually know how to go about protecting themselves against it, or who feel overwhelmed thinking about the overhaul associated with migrating their systems to meet a new set of standards. However, when broken down into smaller steps, the migration process is not so daunting.

Transitioning from cryptosystem to cryptosystem is no trivial task, which is why it is best to start as early as possible. As the NIST National Cybersecurity Center of Excellence (NCCoE) points out: "It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now, so that the information is protected from future attacks."

Switching from one cryptosystem to another within a given security solution is unlikely to be a simple drop-in task, particularly for businesses that haven't even begun planning for the post-quantum transition, which is likely to be the biggest cryptographic transition in decades.

The ease or difficulty with which certain cryptographic algorithms can be switched out in embedded hardware and software will determine the speed with which a transition can be achieved. Crypto-agility allows for a smoother transition between standards. If a system is crypto-agile, it means it is built with flexibility and future-proofing in mind, with cryptographic algorithms easy to update and replace over time with minimal disruption to the overall system.

Taking the next step

Although we don't yet know that a high-functioning quantum computer exists, it is not unfeasible that a bad actor would choose to conceal its existence in order to maintain their technical advantage along with the element of surprise. The prudent way forward is to start preparing for the worst now because it's a question of when, not if.

Post-quantum cryptography standards were announced in July last year. The first draft standards will be published in the next couple of months with the final versions ready in the first half of 2024. In the meantime, it is possible and advised to use hybrid cryptography libraries that can support both classical and post-quantum standards in the transition phase.

In the meantime, businesses can ensure that their cryptography is FIPS 140-3 compliant. FIPS 140-3 is a good stopgap to aim for until more tailored standards are introduced, and because it is a mandatory standard for the protection of sensitive data within US and Canadian federal systems, it is a prerequisite for any contractors that want to do business with these governments.

Another place to look is the Department of Homeland Security, which published a post-quantum cryptography roadmap – a useful guideline for establishing a transition plan before standards are finalised.

The bottom line? The longer organisations wait to act, the greater the potential harm. And since the road to full quantum security will take time, the sooner they begin the transition, the better.

15.How ChatGPT Is Changing The Cybersecurity Game

https://www.helpnetsecurity.com/2023/03/17/chatgpt-cybersecurity-potential/

The cybersecurity industry can leverage GPT-3 potential as a co-pilot to help defeat attackers, according to Sophos.

The latest report details projects developed by Sophos X-Ops using GPT-3's large language models to simplify the search for malicious activity in datasets from security software, more accurately filter spam, and speed up analysis of "living off the land" binary (LOLBin) attacks.

"Since OpenAI unveiled ChatGPT back in November, the security community has largely focused on the potential risks this new technology could bring. Can the AI help wannabee attackers write malware or help cybercriminals write much more convincing phishing emails? Perhaps, but, at Sophos, we've long seen AI as an ally rather than an enemy for defenders, making it a cornerstone technology for Sophos, and GPT-3 is no different. The security community should be paying attention not just to the potential risks, but the potential opportunities GPT-3 brings," said Sean Gallagher, principal threat researcher, Sophos.

ChatGPT cybersecurity potential

Sophos X-Ops researchers, including SophosAI Principal Data Scientist Younghoo Lee, have been working on three prototype projects that demonstrate the potential of GPT-3 as an assistant to cybersecurity defenders. All three use a technique called "few-shot learning" to train the AI model with just a few data samples, reducing the need to collect a large volume of pre-classified data.

The first application Sophos tested with the few-shot learning method was a natural language query interface for sifting through malicious activity in security software telemetry. Sophos tested the model against its endpoint detection and response product. With this interface, defenders can filter through the telemetry with basic English commands, removing the need for defenders to understand SQL or a database's underlying structure.

GPT-3 can simplify certain labor-intensive processes

Next, Sophos tested a new spam filter using ChatGPT and found that, when compared to other machine learning models for spam filtering, the filter using GPT-3 was significantly more accurate.

Finally, Sophos researchers were able to create a program to simplify the process for reverse-engineering the command lines of LOLBins. Such reverse-engineering is notoriously difficult, but also critical for understanding LOLBins' behavior—and putting a stop to those types of attacks in the future.

"One of the growing concerns within security operation centers is the sheer amount of 'noise' coming in. There are just too many notifications and detections to sort through, and many companies are dealing with limited resources. We've proved that, with something like GPT-3, we can simplify certain labor-intensive processes and give back valuable time to defenders. We are already working on incorporating some of the prototypes above into our products, and we've made the results of our efforts available on our GitHub for those interested in testing GPT-3 in their own analysis environments. In the future, we believe that GPT-3 may very well become a standard co-pilot for security experts," said Gallagher.

16.How Will The UK Regulate Quantum Computers?

by Ryan Morrison

https://techmonitor.ai/hardware/quantum/quantum-computer-regulation-uk

In its National Quantum Strategy, which includes £2.5bn of funding, as well as plans for research zones and skills training, the government announced it will establish a regulatory framework "that supports innovation and the ethical use of quantum technologies". This needs to be stable, agile, simple and ethical while also protecting UK capabilities and national security. One expert told *Tech Monitor* the focus should be on legislating for post-quantum cryptography before the UK is left behind.

Quantum computing is a potentially transformative technology, once fully realised it has the potential to change our understanding of the universe, the human brain and tackle problems like climate change. But it also comes with risk, including the potential to easily crack encryption and change warfare.

Governments around the world are investing heavily in quantum technology with China leading the world in terms of direct national-level funding followed by the EU and now the UK. Billions of dollars worth of venture capital, private investment and university research funding are also being put into the technology.

Last year Stanford University's Professor Mauritz Kop declared that we need to learn from our mistakes made around the regulation of AI "before its too late" and said quantum computing has the potential to be "more dangerous than artificial intelligence" without sufficient regulation.

In its National Quantum Strategy the government says it is important to engage early in the debates that will shape the future regulation of quantum technology. Early work will help to identify potential risks with the use of the new technology and develop new shared taxonomies, languages and principles to guide development.

"Eventually new standards, benchmarking and assurance frameworks will increase in importance to facilitate technological development as use cases become more evident, helping to set requirements for interoperability and to measure performance within key sectors," the strategy says.

How the UK will develop ethical quantum systems

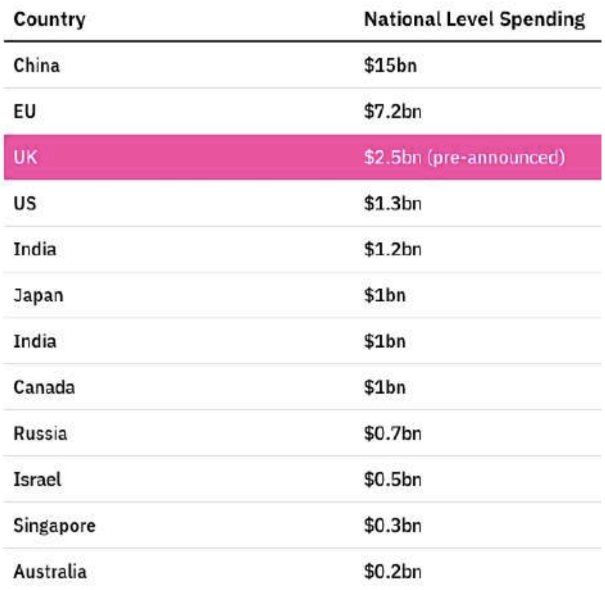
It includes a commitment to put innovation, business growth and the ethical use of quantum technologies at the heart of the UK economy while also trialing technologies within the UK through regulatory testbeds and sandboxes, as well as working with "likeminded partners" around the world to shape norms and standards as the technology evolves and becomes more mainstream.

A lot of the commitment is outward facing, with the strategy calling for the UK to play a role in the World Trade Organisation, the World Economic Forum, the G7, the G20, OECD, NATO, the Council of Europe, the Commonwealth and the UN, including "utilising the UK seat on the International Telecommunications Union (ITU) to ensure that quantum regulation supports UK business and innovation, that the UK's wider prosperity, security and defence interests are represented and that we continue to uphold the UK's values including those on human rights."

The government also outlined proposals to ensure the economy and national security are protected including working with "likeminded allies" to monitor and review current and future controls including through export regimes, security goals and IP protection.

Government's spending billions on quantum computing

The UK ranks third in national-level spending on quantum technology including quantum computing behind China and the EU.



Country	National Level Spending
China	$15bn
EU	$7.2bn
UK	$2.5bn (pre-announced)
US	$1.3bn
India	$1.2bn
Japan	$1bn
India	$1bn
Canada	$1bn
Russia	$0.7bn
Israel	$0.5bn
Singapore	$0.3bn
Australia	$0.2bn

The plan is also to ensure the National Cyber Security Centre (NCSC) continues to publish guidance on the transition to quantum-safe cryptography. "In terms of Government's own preparedness, mitigations have already been put in place for critical information and services," the report declares with specific recommendations to follow the US NIST process.

There will also be work on technical standards, including through quantum safe cryptography in partnership with the ISO, IEC and ITU and efforts on building assurance frameworks for the use of these technologies as they mature. Much of this is following the pattern set out for regulation of artificial intelligence, including sandboxes, standards and regulator-led guidelines.

"The Chancellor bolstered the UK technology strategy with the £2.5bn 'Plan for Quantum', but the writing is on the wall: the extraordinary processing power of quantum computers will have a catastrophic impact on digital systems unless we begin a cryptographic transition now," Tim Callan, chief experience officer at digital identity and security company Sectigo told *Tech Monitor*.

“IT leaders need to start paying attention today to the upcoming threat of quantum computing and preparing their organisations to upgrade to new ‘post quantum’ cryptography in order to head off, or at least mitigate, the damage.”

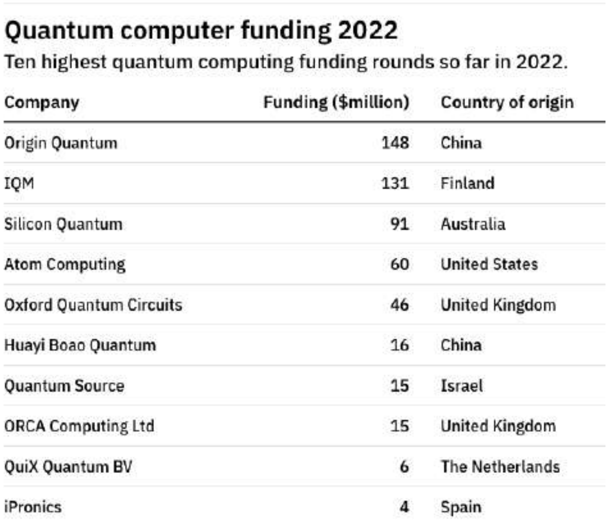
As well as the promise of investment in research, promotion of greater compute power and regulation, the National Quantum Strategy also promises £15m of direct funding to “enable government to act as an intelligent, early customer of quantum technologies,” which James Sanders, principal analyst for cloud and infrastructure at CCS Insight said needs “greater articulation” as currently there are unlikely to be many circumstances where a quantum computer can be used by the government to find efficiency or optimisation that couldn’t be done with a classical machine

Export controls and IP protection for quantum technologies

In terms of regulation, Sanders says it falls under two different priorities: export restriction and intellectual property protection. The first is similar to the approach seen with the export of precision semiconductor manufacturing technology as well as export of advanced GPUs for AI model training, which he says are “two aspects prioritised today by the US government.”

Ben Packman, head of strategy at UK post-quantum cryptography company, PQShield, says quantum technology is developing at speed around the world, and that more up-front funding will be required for the UK to maintain its leadership position in the sector. “Any delays could leave the door open for others to overtake us, which is a real problem if you’re thinking about the UK’s adversaries developing a quantum computer intended for malicious purposes,” he says.

Private and public partnerships are required to protect against this, and other risks associated with the technology, including the adoption of legislative and policy updates. The US has the Quantum Computing Cybersecurity Preparedness Act but, in the UK, this new strategy is “light when it comes to mitigating the risks associated with quantum,” says Packman.



Quantum computer funding 2022

Ten highest quantum computing funding rounds so far in 2022.

Company	Funding ($million)	Country of origin
Origin Quantum	148	China
IQM	131	Finland
Silicon Quantum	91	Australia
Atom Computing	60	United States
Oxford Quantum Circuits	46	United Kingdom
Huayi Boao Quantum	16	China
Quantum Source	15	Israel
ORCA Computing Ltd	15	United Kingdom
QuiX Quantum BV	6	The Netherlands
iPronics	4	Spain

He said that while regulators are already engaging with industry and academics across the quantum value chain to build a regulatory framework, the UK is behind when it comes to cryptography legislation. “The US has already actively legislated for quantum-safe cryptography, and where the US National Security Agency (NSA) has issued a very specific set of guidance and timelines in its CNSA 2.0 framework," he says. "We’d like to see the UK match and even go beyond this if it is to become a true quantum superpower.”

Many British companies, including PQShield, are contributing to the cryptographic standards considered as part of the NIST review. The outcome of this will set the global standard for post-quantum cryptography, including algorithms used across industry and government.

“We’d like to see the UK’s quantum achievements shouted about from the very top,” Packman adds. “The government also needs to align all its departments on the same path, including bodies like GCHQ and the National Cyber Security Centre (NCSC) and MI5’s newly-created National Protective Security Authority (NPSA).

"The strategy doesn’t mention the DRCF or Digital Catapult and how they can support the wider quantum strategy. It seems to me that both schemes could play a relevant role, so it would be good to see the dots being connected at a strategic level.”

17.Mathworks Introduces A Matlab Support Package For Quantum Computing That Can Run Circuits On Amazon Braket

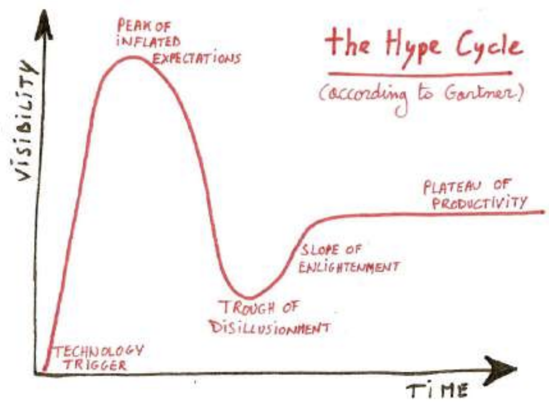
https://quantumcomputingreport.com/mathworks-introduces-a-matlab-support-package-for-quantum-computing-that-can-run-circuits-on-amazon-braket/

The MATLAB Support Package for Quantum Computing allows users to build, simulate, and run quantum algorithms for prototyping quantum programs. It will allow a user to input a quantum program and then do a local simulation to display the results and includes additional capabilities to plot a histogram, display state formulas, and query possible states. A key feature is that it will also allow a user to run their quantum circuit on one of the several quantum processors or high performance quantum simulators that are available on Amazon Braket for those who have an AWS account with access to Amazon Braket. For more information about this new package, you can view a web page for it here and also a page with instructions on how to set it up and use it here.

18.The Real Danger Of The Quantum Hype-Cynicism Cycle

by Matt Swayne
https://thequantuminsider.com/2023/03/16/tqi-opinion-the-real-danger-of-the-quantum-hype-cynicism-cycle/

Quantum technology, devices that rely on quantum mechanics for computation, sensing and a range of other applications, may have achieved hype status faster than any other previous technological wave. The glittering quantum computer chandelier adorning the Jan. 26 Time Magazine cover story on quantum might be a trophy of the technology's record-setting hype status.



The oft-cited, yet poorly defined *hype cycle* has become integral to media conversations surrounding the introduction of new technologies. These discussions, once civil and productive, are now more likely to rise to the level of ad hominem attacks that are counterproductive to the long-term success of what could be an important tool for everything from non-satellite navigation to personalized medicine. National security also hangs in the balance.

First, let's try to de-hype the hype cycle itself. The hype cycle is most famously exemplified by the Gartner Hype Cycle, however, recently the tag has been decoupled from that methodology to refer to any wave of interest in a technology. In truth, though, this cycle of rising and waning excitement can better be explained as a typical wave of human interest and focus. In the short term, we can see the phenomena play out in news cycles, for example. News stories – from celebrity deaths to future quantum hacking – follow a typical pattern that rapidly peaks in interest, often drowning out other – more important – issues. Eventually, those stories, which once riveted the general audience, begin to wane, settling into not a trough not of disillusionment, but of fickle disinterest. Longer term, we see similar patterns in everything from protest movements to musical fads.

Both the inflated expectations and — importantly — the depths of disillusionment have little to do with the intrinsic value of the technology itself, or its future potential. Exposing the hype cycle to be simply normal human information processing may seem to be merely one of semantics, but the hype moniker is problematic for a few reasons, particularly in the science and technology field.

Hype, Cynicism and National Security

First, there is an intentionality in the term, hype. In other words, a technology must be hyped by someone. Hype is also conspiratorial. Usually it's not just someone who is hyping an emerging technology — for example, a quantum computer — but a nefarious unseen cabal of "someones" actively hyping the technology out of self-interest.

Therein lies the potential for long-term damage to quantum efforts. Just as this is a hype cycle, it can swiftly turn into a cynicism cycle. A cabal of hypers who point out every success and gloss over technical challenges ahead will likely inspire a cabal of de-hypers who make an effort to decry the technical challenges as impossible and attempt to quash real advances and well-intentioned hope for success.

Because human interest and focus is nearly as vulnerable as those superconducting qubits resting isolated in the golden chandelier, hype eventually fades, quite possibly leaving not disillusionment, but a deep distrust and cynicism in quantum technology. What must be emphasized is that tomorrow's wallowing quantum cynicism is no more supported in facts than the mad peak of quantum hype we are allegedly experiencing today.

The danger is a quantum winter settles in, funding dries up, investments meander into other fields and research areas, until ultimately, quantum is reduced to a ground state.

Good, the quantum cynics may cry, attributing the demise to the natural consequences of the quantum hype machine. But this hype-cynicism wave is different for quantum. There is simply too much riding on the success of quantum technology to allow it to fade away and spend a decade or two in a trough of research disillusionment before gradually regaining traction. Quantum technology holds in its grasp key elements of national security, such as the ability to shred current data security protocols and achieve precise navigation for military vehicles even when satellites are jammed.

On the other hand, autocratic regimes are not swayed by public opinion, Twitter flaming or LinkedIn shaming. They can afford to invest in research in steady or increasing amounts. The geopolitical balance literally could be held by the thread of the findings in a single study or the revelation of an obscure experiment.

That's what's at stake. So what do we do?

How We Can Break The Tech-Hype-Cynicism Cycle

We humans are typically not good at predicting what technologies will work. Thomas Watson, president of IBM famously contested that "I think there is a world market for maybe five computers" in 1943. Often blinded by cognitive biases, academic grudges and ideological differences, past technological hypers and haters alike have demonstrated the difficulty of accurately predicting the achievement – let alone the timeline and impact – of emerging technologies. Consider Albert Einstein, who some call the father of nuclear energy, initially didn't believe nuclear power was even possible, adding, "There is not the slightest indication that nuclear energy will ever be attainable. It would mean the atom would have to be shattered at will." In computing, that crystal ball is even easier to shatter. In 1998, Paul Krugman, renowned economist, said, "The internet will fade away because most people have nothing to say to each other. By 2005 it will be clear that the internet's impact on the global economy has been no greater than the fax machine."

We propose there are several ways of breaking the Tech-Hype-Cynicism cycle.

Most importantly, we need better data. Between 2019 and 2022 we estimate that 30 new quantum computing hardware companies were founded, each pursuing slightly different aims and technologies. Before we start calling out dead-ends we need to have a holistic understanding of the myriad paths being pursued. In markets where intellectual property is jealously protected and national security interests abound, we must make use of the best open source intelligence available. At Resonance we believe that insights into the state of the market can be found in the relationships and partnerships being built between organizations. We may not be able to understand every business, but we can extract insights from hotspots of research and collaboration.

Secondly we need smarter science communication strategies and more realistic expectation setting.

Better data should ease confusion about what might be the most complex technology ever created. But, the latest science communication research also suggests that we need to discuss the latest findings on quantum research in clear and convincing ways. Messages based on greed and fear and driven by divisive social media posturing will only cause deeper fissures between people who are actually on the same team.

Thirdly, we need to work together. Quantum critics and quantum promoters can form unstoppable teams that balance realism with optimism to build quantum technology that works for all and quantum technology that works for good.

Within a few short years, quantum technology has gone from science fiction to popular science. Its fast ascent has intensified the hype-cynicism cycle for this technology. Without a deeper understanding of the space and proper and realistic communication about its potential, quantum computing could join a list of scientific issues – from vaccinations to climate change – that are clouded and crippled by irrational exuberance and irresponsible cynicism.

Maybe we can't create an eternal quantum spring, but perhaps we can make sure quantum winter is short and mild.

19.SemiQon To Develop Affordable And Scalable Quantum Computers

by Carolyn Mathas
https://quantumcomputingreport.com/semiqon-to-develop-affordable-and-scalable-quantum-computers/

VTT Technical Research Centre of Finland just launched quantum computing spinout SemiQon with a mission to power the scale up of quantum computers with silicon-based quantum processors. This new quantum processor chip is made from silicon semiconductors versus a variety of non-standard materials. In this case, the use of easy-to-replicate silicon quantum dot-based technology provide both scalability and manufacturability, while functioning at warmer temperatures for greater operability and sustainability. According to SemiQon, this capability could enable quantum processors requiring millions of qubits for fault-tolerant operation. And, in order to tackle truly complex problems, quantum computers will need to operate with millions of qubits instead of hundreds of qubits available today.

Himadri Majumdar, SemiQon's CEO, says that the solution addresses three challenges that currently slow down quantum computer development globally–scalability, price and sustainability. Lowering cost includes the large-scale manufacturing processes and facilities already exist for silicon and SemiQon currently operates in such a pilot manufacturing facility in Finland. The use of inexpensive quantum dot technology, and warmer-temperature operation that requires a fraction of the energy currently used by competing solutions all contribute to lower cost and sustainability.

Voima Ventures is backing the development of quantum computer chips that will result in future quantum computers being more affordable and scalable. According to Jussi Sainiemi, partner at Voima Ventures, most quantum investments have addressed superconducting and other qubit approaches, leaving silicon semiconductor qubit technology underfunded. Silicon, however, is not burdened with the scalability challenges inherent in the other solutions.

SemiQon officially began post-spinout operations in February 2023.

20.Quantum Computing Is The Future, And Schools Need To Catch Up

by Olivia Lanes
https://www.scientificamerican.com/article/quantum-computing-is-the-future-and-schools-need-to-catch-up/

The harnessed power of the subatomic world could soon upend the modern computing industry. Quantum computers are all over the news, and fundamental work on the theory that gave rise to them even won last year's Nobel Prize.

But the one place you might not hear about them is inside a physics classroom. And if we have any hope of creating a technology-literate population and developing a workforce for this emerging field, that needs to change.

What's a quantum computer? Unlike the computer sitting on your desk, which encodes words or numbers as collections of 1s and 0s called "bits," quantum computers rely on quantum bits or "qubits," which are more, well, dicey (much to Einstein's chagrin). Unlike bits, qubits assign weights to their 1s and 0s, more like how you would tailor loaded dice, which means there is a probability associated with measuring either number. They lack a definite value, instead embodying a bit of both states until you measure them. Quantum algorithms run on these qubits, and, theoretically, perform calculations by rolling these loaded dice, causing their probabilities to interfere and increasing their odds of finding the ideal solution. The ultimate hope is that math operations such as factoring gargantuan numbers, which now would take a computer billions of years to perform, would only take a few days on a quantum computer.

This new way of computing could crack hard problems that are out of reach for classical processors, opening new frontiers everywhere from drug discovery to artificial intelligence. But rather than expose students to quantum phenomena, most physics curricula today are designed to start with the physics ABCs—riveting topics such as strings on pulleys and inclined planes—and while students certainly need to know the basics (there's room for Newton and Maxwell alongside Schrödinger's cat), there should to be time spent connecting what they are learning to state-of-the-art technology.

That matters because quantum computing is no longer a science experiment. Technology demonstrations from IBM (my employer), Google and other industry players prove that useful quantum computing is on the horizon. The supply of quantum workers however, remains quite small. A 2021 McKinsey report predicts major talent shortages—with the number of open jobs outnumbering the number of qualified applicants by about 3 to 1—until at least the end of the decade without fixes. That report also estimates that the quantum talent pool in the U.S. will fall far behind China and Europe. China has announced the most public funding to date of any country, more than double the investments by E.U. governments, $15.3 billion compared to $7.2 billion, and eight times more than U.S. government investments.

Thankfully, things are starting to change. Universities are exposing students sooner to once-feared quantum mechanics courses. Students are also learning through less-traditional means, like YouTube channels or online courses, and seeking out open-source communities to begin their quantum journeys. And it's about time, as demand is skyrocketing for quantum-savvy scientists, software developers and even business majors to fill a pipeline of scientific talent. We can't keep waiting six or more years for every one of those students to receive a Ph.D., which is the norm in the field right now.

Schools are finally responding to this need. Some universities are offering non-Ph.D. programs in quantum computing, for example. In recent years, Wisconsin and the University of California, Los Angeles, have welcomed inaugural classes of quantum information masters' degree students into intensive year-long programs. U.C.L.A. ended up bringing in a much larger cohort than the university anticipated, demonstrating student demand. The University of Pittsburgh has taken a different approach, launching a new undergraduate major combining physics and traditional computer science, answering the need for a four-year program that prepares students for either employment or more education. In addition, Ohio recently became the first state to add quantum training to its K-12 science curricula.

And finally, professors are starting to incorporate hands-on, application-focused lessons into their quantum curricula. Universities around the world are beginning to teach courses using Qiskit, Cirq and other open-source quantum programming frameworks that let their students experiment on real quantum computers through the cloud.

Some question this initiative. I've heard skeptics ask, is it a good idea to train a new generation of students in a technology that is not fully realized? Or what can really be gained by trying to teach quantum physics to students so young?

These are reasonable questions but consider: Quantum is more than just a technology; it's a field of study that undergirds chemistry, biology, engineering and more; quantum education is valuable beyond just computing. And if quantum computing does pan out—which I think it will—then we'll be far better off if more people understand it.

Quantum technology is the future, and quantum computing education *is* STEM education, as Charles Tahan, the director at the National Quantum Coordination Office, once told me. Not all of these students will end up directly in the quantum industry at the end, and that's all for the better. They might work in a related science or engineering field, such as fiber optics or cybersecurity, that would benefit from their knowledge of quantum, or in business where they can make better decisions based on their understanding of the technology.

At my job, I talk about quantum technologies to students daily. And I've learned that above all, they are hungry to learn. Quantum overturns our perception of reality. It draws people in and keeps them there, as the popularity of NASA and the moon landing did for astrophysics. We should lean into what captures students' attention and shape our programs and curricula to meet these desires.

For those schools adapting to the emerging quantum era, the core message is simple: don't underestimate your students. Some might hear the word quantum and shudder, fearing it is beyond their comprehension. But I have met high school and middle school students who grasp the concepts with ease. How can we expect young students to pursue this subject when we gate-keep it behind years of pulleys and sliding blocks? Universities should start introducing quantum information much sooner in the curriculum, and K-12 schools should not shy away from introducing some basic quantum concepts at an early age. We should not underestimate students, but rather, we should trust them to tell us what they want to learn—for their benefit and for all of science. If we drag our feet even a little, we all stand to lose the immense benefits quantum could bring to our economy, technology and future industries.

21.GAO Offers Quantum Guidance To Federal Agencies

by Alexandra Kelley

https://www.nextgov.com/emerging-tech/2023/03/gao-offers-quantum-guidance-federal-agencies/383947/

More federal guidance has emerged as the world continues its preparations for the advent of quantum computing with the Government Accountability Office disseminating fast facts on how to secure sensitive data in a post-quantum cryptographic world.

In its March 8 advisory, GAO highlights how vulnerable current classical encryption algorithms could be to those operating within a quantum computer. These vulnerabilities, combined with more cyberattacks that work to hack and harvest data, prompted the GAO to offer guidance on implementing post-quantum cryptography measures.

"The mathematical structure underlying current encryption methods commonly used for public-key cryptography and digital signatures could be broken with a CRQC [cryptographically relevant quantum computers]," the report reads.

Despite the estimated timeline for a viable quantum computer to become operational in no less than a decade, expert organizations are working to fortify U.S. digital networks well before they are susceptible to a quantum algorithm's powerful decryption capabilities. This is generally accomplished through quantum-resilient algorithms, with the National Institute of Standards and Technology spearheading their development since 2016.

GAO authors break down the cybersecurity and encryption needs for classical systems in a post-quantum world. Explaining that the expert consensus suggests private key encryptions strategies are less susceptible to attacks by quantum computers.

"The mathematical structure underlying current encryption methods commonly used for public-key cryptography and digital signatures could be broken with a CRQC," the report says.

One recommended algorithm is Lattice-based encryption, which is harder to decrypt because it functions in a multidimensional space using geometry to secure data.

The White House has currently set a deadline for all federal entities to transition to post-quantum cryptography standards by 2035. In President Joe Biden's new national strategy, quantum cryptography plays a role in modern cybersecurity principles.

Aside from implementing new, updated algorithms, the report also recommends updating digital infrastructures and enhanced data security are two steps to preemptively secure data networks.

22.Understanding Password Behavior Key To Developing Stronger Cybersecurity Protocols

https://www.helpnetsecurity.com/2023/03/13/understanding-password-behavior/

Passwords are still the weakest link in an organization's network, as proven by the analysis of over 800 million breached passwords, according to Specops Software.

The study found 88% of passwords used in successful attacks consisted of 12 characters or less, with the most common being 8 characters (24%).

The most common base terms used in passwords were: 'password', 'admin', 'welcome' and 'p@ssw0rd'.

Passwords containing only lowercase letters were the most common character combination found, making up 18.82% of passwords used in attacks.

The sophistication of modern password attacks

Ironically, the study revealed that 83% of compromised passwords did satisfy both length and complexity requirements of cybersecurity compliance standards such as NIST, PCI, ICO for GDPR, HITRUST for HIPAA and Cyber Essentials for NCSC.

"This shows that while organizations are making concerted efforts to follow password best practices and industry standards, more needs to be done to ensure passwords are strong and unique," said Darren James, product manager at Specops Software.

“With the sophistication of modern password attacks, additional security measures are always required to protect access to sensitive data,” James continued.

Furthermore, brute force attacks are a common tactic used by cybercriminals to gain access into an organization’s network to steal sensitive data. Threat actors will use common, probable, and even breached passwords to systematically run them against a user’s email to gain access to a given account.

For example, the Specops researchers also noticed the inclusion of ‘homelesspa’ – a password term found in 2016 MySpace data leak, proving that ‘old’, breached password terms are still being leveraged by hackers many years later.

This is a critical reason why organizations need strong password policy enforcement.

Strong password policy enforcement

In Nvidia’s data breach in 2022, where thousands of employee passwords were leaked, many employees had used passwords such as ‘Nvidia’, ‘qwerty’ and ‘nvidia3d’.

Having passwords related to the organization is an easy route for hackers into the network. Despite industry warnings against easily guessable passwords, users still resort to common passwords.

“The 2023 edition of the Weak Password Report reiterates the ongoing challenges of securing the weakest link in the enterprise IT environment,” said James. “To stay on top of today’s credential attacks, all companies should put strong password policy enforcement in place, including custom dictionaries related to the organization.”

Even with end-user training, password reuse and other risky practices are all too common.

23.QuSeCure Launches Live End-To-End Satellite Quantum Resilient Link Through Space

https://www.helpnetsecurity.com/2023/03/11/qusecure-quantum-resilient-cryptographic-communications-satellite-link/

QuSecure has accomplished the first known live, end-to-end quantum-resilient cryptographic communications satellite link through space, marking the first time U.S. satellite data transmissions have been protected from classical and quantum decryption attacks using post-quantum cryptography (PQC).

The quantum-secure communication to space and back to Earth was made through a Starlink satellite working with a leading Global System Integrator (GSI) and security provider. Starlink is a satellite internet constellation operated by SpaceX consisting of more than 3,500 small satellites in low Earth orbit (LEO) which communicate with designated ground transceivers to provide satellite Internet access coverage to more than 45 countries.

Data shared between satellites and ground stations travels through the air and traditionally has been vulnerable to theft, leaving satellite communications even more accessible than typical internet communications. Now with QuSecure, any Federal and commercial organization can conduct live, secure, classical- and quantum-safe communications and data transmissions through space.

This enables servers, edge, IoT, battlefield, and other devices outside conventional data networks to adopt quantum-safe communications. From secure military communications to financial payment and data transmissions, organizations now can be fully protected from data harvesting. Data harvested today could be decrypted by a quantum computer in the future, an active and ongoing practice known as Steal Now Decrypt Later (SNDL).

“QuSecure’s breakthrough in secure satellite communications capabilities creates the world’s first extraterrestrial post-quantum resilient communications mesh; and is a very important step in our collective journey toward quantum safety,” said Aaron Moore, QuSecure’s EVP, Head of Engineering.

“Our control plane gives customers the ability to make simple upgrades to legacy encryption without ‘rip and replace’ measures – all with less than 0.1 seconds of latency. By putting our customers first, our aim is to assure private and safe communication, anytime, anywhere, on any device. Achieving this milestone is a giant leap forward for QuSecure in fulfilling our corporate mission to ensure an exceptionally secure future,” added Moore.

“Starlink’s base of over a million subscribers speaks not just to its considerable strength as a company but to LEO’s attractiveness as a constellation layer,” said Lisa Hammitt, QuSecure Board Director. “With QuSecure already leading a new class of cryptography terrestrially, it only makes sense that LEO — and Starlink in particular — would host its first quantum channel in space.”

During this secure satellite communications test on the Starlink network, QuSecure successfully sent quantum-resilient data from their Quark server through labs at Rearden Logic in Colorado to a Starlink terminal. Next, QuSecure sent the signal via uplink to a Starlink satellite and then via downlink back to Earth.

All communications in these sessions were secured using QuSecure’s Quantum Secure Layer (QSL) protecting all data in transit with post-quantum cybersecurity. QuSecure’s unique solution creates a secure quantum tunnel that protects the transmitted data from both classical and post-quantum decryption. Before this achievement, data from satellites could be collected and potentially broken by classical means and most certainly by quantum computers with enough power.

QuProtect software enables organizations to leverage quantum-resilient technology to prevent today’s cyberattacks, while future-proofing networks and preparing for quantum cyberthreats. It provides quantum-resilient cryptography, anytime, anywhere and on any device.

QuProtect software uses an end-to-end quantum-security-as-a-service architecture that addresses the digital ecosystem’s most vulnerable aspects, uniquely combining zero-trust, next-generation post-quantum-cryptography, crypto agility, quantum-strength keys, high availability, easy deployment, and active defense into a comprehensive and interoperable cybersecurity suite. The end-to-end approach is designed to protect the entire information lifecycle as data is communicated, used and stored.

Using QuProtect, an organization can implement PQC across all devices on the network with minimal disruption to existing systems, protecting against current classical and future quantum attacks which could irreparably disrupt industries and infrastructures across government and commercial sectors, at the same time solving today’s complex compliance challenges, such as bring-your-own-device (BYOD) and work-from-home policies.

24.It's A Weird, Weird Quantum World

by Jennifer Chu
https://news.mit.edu/2023/weird-weird-quantum-world-peter-shor-killian-lecture-0310

In MIT's 2023 Killian Lecture, Peter Shor shares a brief history of quantum computing from a personal viewpoint.

In 1994, as Professor Peter Shor PhD '85 tells it, internal seminars at AT&T Bell Labs were lively affairs. The audience of physicists was an active and inquisitive bunch, often pelting speakers with questions throughout their talks. Shor, who worked at Bell Labs at the time, remembers several occasions when a speaker couldn't get past their third slide, as they attempted to address a rapid line of questioning before their time was up.

That year, when Shor took his turn to present an algorithm he had recently worked out, the physicists paid keen attention to Shor's entire talk — and then some.

"Mine went pretty well," he told an MIT audience yesterday.

In that 1994 seminar talk, Shor presented a proof that showed how a quantum system could be applied to solve a particular problem more quickly than a classical computer. That problem, known as the discrete logarithm problem, was known to be unsolvable by classical means. As such, discrete logarithms had been used as the basis for a handful of security systems at the time.

Shor's work was the first to show that a quantum computer could solve a real, practical problem. His talk set the seminar abuzz, and the news spread, then became conflated. Four days after his initial talk, physicists across the country were assuming Shor had solved a related, though much thornier problem: prime factorization — the challenge of finding a very large number's two prime factors. Though some security systems employ discrete logarithms, most encryption schemes today are based on prime factorization and the assumption that it is impossible to crack.

"It was like the children's game of 'telephone,' where the rumor spread that I had figured out factoring," Shor says. "And in the four days since [the talk], I had!"

By tweaking his original problem, Shor happened to find a similar quantum solution for prime factorization. His solution, known today as Shor's algorithm, showed how a quantum computer could factorize very large numbers. Quantum computing, once thought of as a thought experiment, suddenly had in Shor's algorithm an instruction manual for a very real, and potentially disruptive application. His work simultaneously ignited multiple new lines of research in quantum computing, information science, and cryptography.

The rest is history, the highlights of which Shor recounted to a standing-room-only audience in MIT's Huntington Hall, Room 10-250. Shor, who is the Morss Professor of Applied Mathematics at MIT, spoke as this year's recipient of the James R. Killian, Jr. Faculty Achievement Award, which is the highest honor the Institute faculty can bestow upon one of its members each academic year.

In introducing Shor's talk, Lily Tsai, chair of the faculty, quoted the award citation:

"Without exception, the faculty who nominated him all commented on his vision, genius, and technical mastery, and commended him for the brilliance of his work," Tsai said. "Professor Shor's work demonstrates that quantum computers have the potential to open up new avenues of human thought and endeavor."

A quantum history

During the one-hour lecture, Shor took the audience through a brief history of quantum computing, peppering the talk with personal recollections of his own role. The story, he said, begins in the 1930s with the discovery of quantum mechanics — the physical behavior of matter at the smallest, subatomic scales — and the question that soon followed: Why was quantum so strange?

Physicists grappled with the new description of the physical world, which was so different from the "classical" Newtonian mechanics that had been understood for centuries. Shor says that the physicist Erwin Schrödinger attempted to "illustrate the absurdity" of the new theory with his now-famous thought experiment involving a cat in a box: How can it embody both states — dead and alive? The exercise challenged the idea of superposition, a key property of quantum mechanics that predicts a quantum bit such as an atom should hold more than one state simultaneously.

Spookier still was the prediction of entanglement, which posed that two atoms could be inextricably linked. Any change to one should then affect the other, no matter the distance separating them.

"Nobody considered using this strangeness for information storage, until Wiesner," Shor said.

Wiesner was Stephen Wiesner, who in the late 1960s was a graduate student at Columbia University who was later credited with formulating some of the basic principles of quantum information theory. Wiesner's key contribution was a paper that was initially spurned. He had proposed a way to create "quantum money," or currency that was resistant to forgery, by harnessing a strange property in which quantum states cannot be perfectly duplicated — a prediction known as the "no-cloning" theorem.

As Shor remembers it, Wiesner wrote out his idea on a typewriter, sent it off for consideration by his peers, and was roundly rejected. It wasn't until another physicist, Charles Bennett, found the paper, "pulled it out of a drawer, and got it published," solidifying Wiesner's role in quantum computing's history. Bennett went further, realizing that the basic idea of quantum money could be applied to develop a scheme of quantum key distribution, in which the security of a piece of information, such as a private key passed between parties, is protected by another weird quantum property.

Bennett worked out the idea with Gilles Brassard in 1984. The BB84 algorithm was the first protocol for a crypto system that relied entirely on the weird phenomena of quantum physics. Sometime in the 1980s, Bennett came around to Bell Labs to present BB84. It was Shor's first time hearing of quantum computing, and he was hooked.

Shor initially tried to work out an answer to a question Bennett posed to the audience: How can the protocol be proven mathematically to indeed be secure? The problem, however, was too thorny, and Shor abandoned the question, though not the subject. He followed the efforts of his colleagues in the growing field of quantum information science, eventually landing on a paper by physicist Daniel Simon, who proposed something truly weird: that a system of quantum computing bits could solve a particular problem exponentially faster than a classical computer.

The problem itself, as Simon posed it, was an esoteric one, and his paper, like Wiesner's, was initially rejected. But Shor saw something in its structure — specifically, that the problem related to the much more concrete problems of discrete logarithms and factoring. He worked from Simon's starting point to see whether a quantum system could solve discrete logarithms more quickly than a classical system. His first attempts were a draw. The quantum algorithm solved a problem just as fast as its classical counterpart. But there were hints that it could do better.

“There’s still hope in trying,” Shor remembers thinking.

When he did work it out, he presented his algorithm for a quantum discrete log algorithm in the 1994 symposium at Bell Labs. In the four days since his talk, he managed to also work out his eponymous prime factorization algorithm.

The reception was overwhelming but also skeptical, as physicists assumed that a practical quantum computer would instantly crumble at the barest hint of noise, resulting in a cascade of errors in its factoring computation.

“I worried about this problem,” Shor said.

So, he again went to work, looking for a way to correct errors in a quantum system without disturbing the state of the computing quantum bits. He found an answer through concatenation, which broadly refers to a series of interconnected events. In his case, Shor found a way to link qubits, and store the information of one logical, or computing qubit among nine highly entangled, physical qubits. In this way, any error in the logical qubit can be measured and fixed within the physical qubits, without having to measure (and therefore destroy) the qubit involved in the actual computation.

Shor’s new algorithm was the first quantum error correcting code that proved a quantum computer could be tolerant to faults, and therefore a very real possibility.

“The world of quantum mechanics is not the world of your intuition,” Shor said in closing his remarks. “Quantum mechanics is the way the world really is.”

Quantum’s future

Following his talk, Shor took several questions from the audience, including one that drives a huge effort in quantum information science today: When will we see a real, practical quantum computer?

To factor a large number, Shor estimates that a quantum system would require at least 1,000 qubits. To factor the very large numbers that underpin today’s internet and security systems would require millions of qubits.

“That’s going to take a whole bunch of years,” Shor said. “We may never make a quantum computer, ever… but if someone has a great idea, maybe we could see one 10 years from now.”

In the meantime, he noted that, as work in quantum computing has ballooned in recent years, so has work toward post-quantum cryptography and efforts to develop alternative crypto systems that are secure against quantum-based code cracking. Shor compares these efforts to the scramble leading up to “Y2K,” and the prospect of a digital catastrophe at the turn of the last century.

“You probably should have started years ago,” Shor said. “If you wait until the last minute, when it’s clear quantum computers will be built, you will probably be too late.”

Shor received his PhD from MIT in 1985, and went on to complete a postdoc at the Mathematical Sciences Research Institute at Berkeley, California. He then spent several years at AT&T Bell Labs, and then at AT&T Shannon Labs, before returning to MIT as a tenured faculty member in 2003.

Shor’s contributions have been recognized by numerous awards, most recently with the 2023 Breakthrough Prize in Fundamental Physics, which he shared with Bennett, Brassard, and physicist David Deutsch. His other accolades include the MacArthur Fellowship, the Nevanlinna Prize (now the IMU Abacus Medal), the Dirac Medal, the King Faisal International Prize in Science, and the BBVA Foundation

Frontiers of Knowledge Award. Shor is a member of the National Academy of Sciences and the American Academy of Arts and Sciences. He is also a fellow of the American Mathematical Society and the Association for Computing Machinery.

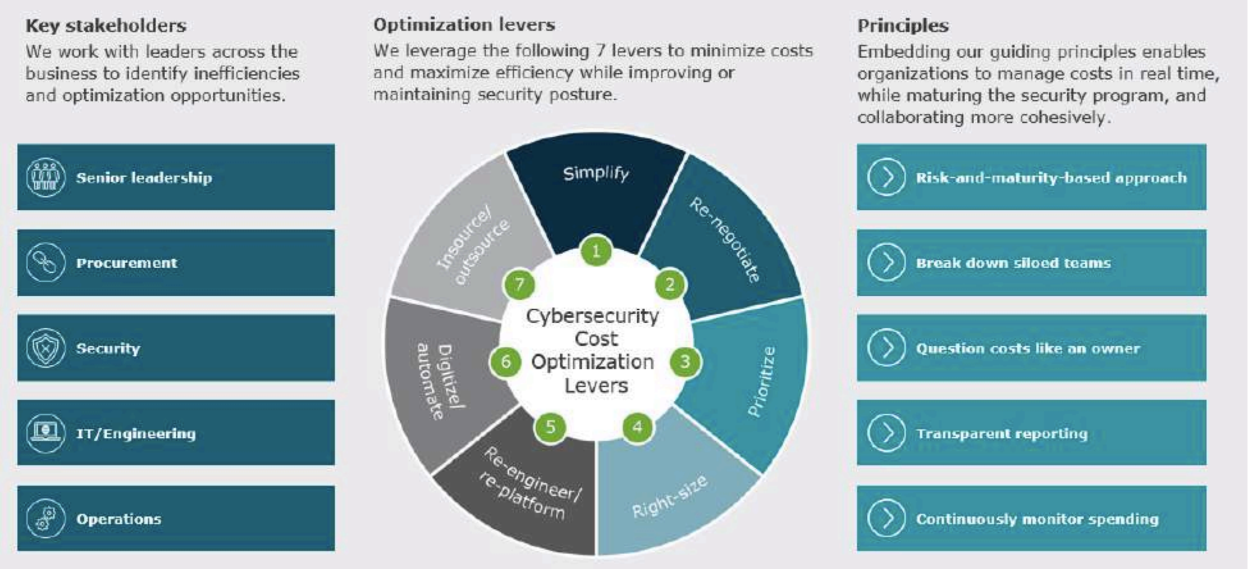
25.Seven levers to optimize cybersecurity cost and balance security needs

by Megha Kalsi and Lukas Weber
https://insights.alixpartners.com/post/102i9vt/seven-levers-to-optimize-cybersecurity-cost-and-balance-security-needs

There are many security leaders across the globe that experience the hardship of budget reduction every year or during uncertain times for the business. Not only that, but these leaders are also given the responsibility to either maintain the security program in its current state or told to improve the security maturity of the program with budget cuts.

You might ask yourself, why would a business cut costs in cybersecurity when it is considered a top priority for most organizations and boards? Some contributing factors include C-Suite changes, uncontrolled cost, but the most common reason nowadays is the anticipation of a downturn in the global economy.

Although these situations may not be ideal, all is not lost. There are ways to optimize cybersecurity cost without completely compromising an organizations overall security posture. We examine seven levers that can be pulled during times of economic uncertainty to minimize costs, without compromising security.


Key stakeholders
We work with leaders across the business to identify inefficiencies and optimization opportunities.

Optimization levers
We leverage the following 7 levers to minimize costs and maximize efficiency while improving or maintaining security posture.

Principles
Embedding our guiding principles enables organizations to manage costs in real time, while maturing the security program, and collaborating more cohesively.

AlixPartners Cybersecurity Cost Optimization Framework

What are the levers of cybersecurity cost optimization?

Cybersecurity programs are known to cost organizations money and are deemed as “non-revenue generating”. On the flip side, a cybersecurity program is pivotal to organizations and help save millions, and in some cases, billions of dollars in fines, breach costs, lawsuits, and much more. Here are seven cybersecurity cost optimization levers a company can implement without compromising security:

1. Simplify

Simplifying cybersecurity may sound like an insurmountable task to most cybersecurity professionals but the reality is, it’s doable. “Simplify” means cutting down or reducing, which requires us to assess what we currently have and take action to make a change. Some steps that can be taken to simplify a cybersecurity program include assessing the current cybersecurity tool stack and vendor contracts, centralizing security insights, and revisiting the operating model.

In order to not compromise security, organizations must categorize the tools in the existing stack as “required”, “nice to have”, “can be eliminated”. If a security tool is deemed “required”, that means the removal of the tool would compromise the overall security of the organization and the features cannot be substituted by another tool (Additional information regarding tools rationalization can be found in the “right-size” lever below). A similar exercise can be done with the list of cybersecurity vendors. Additionally, centralizing logs and eliminating unused log types can reduce storage costs and provide the security team with more valuable insights to address potential attacks.

Further, revisiting the operating model not only helps to simplify technology, but also the people and processes; and ultimately reduces costs. Cybersecurity leaders should ask themselves “Which skills do we need on our cybersecurity team?”; “Do we have the right resources, in the right places, doing the right things?”; “Will there be an impact on the security posture if we update the organizational structure?”

2. Renegotiate

As Chester Karrass once said, “In Business, you don’t get what you deserve, you get what you negotiate”. Negotiating, or in this case “Re-negotiating” requires cybersecurity programs to review existing vendor contracts and identify options that can reduce overall costs. This does not mean that services and products need to be eliminated. It means the agreement requires updates to potentially get more for less. This involves identifying vendors that provide products and services and discussing if they can do better.

For example, if a cybersecurity program decides to eliminate a security tool that was being managed internally; can the existing Managed Security Service Provider fill the security gap without raising the cost or minimally increasing the cost of the current agreement?

Cybersecurity organizations should revisit vendor agreements to seek better terms by updating contract language and adding specific Service Level Agreements that may have been broad initially. As a result, the information provided by these vendors become meaningful and may fill an existing security visibility and security capability gaps. Re-negotiating does not mean cybersecurity programs will become immature. It can result in cybersecurity programs tightening their expectations, increasing services, and gaining better insights.

3. Prioritize

Organizations cannot employ effective security practices without robust risk management in place. Measuring risks in terms of annualized loss expectancy is integral to the process. Prioritizing security investments based on the reduction in the organization's annualized loss expectancy minimizes expenditure on unnecessary controls, while delivering the highest return on security investment.

A prerequisite to effective investment prioritization is an understanding of the value of the assets which the organization is protecting. Weighing investment decisions against the value of the assets prevents the implementation of measures which can be more costly than the value of the asset the measures are designed to protect.

4. Right-size

Technological controls are the answer to some, but not all, problems. Often, security functions adopt a technology-oriented approach to mitigating risks, which can lead to an overabundance in tooling and licensing.

Right-sizing is the process of identifying overlapping security capability by interviewing security teams and examining available tooling. Often, siloed security teams duplicate effort and don't tend to use all tooling available to them, which presents rationalization opportunities.
How does reducing the resources available to the security function impact defense in depth? The distinction between technological solutions that are almost identical in capability and layering distinct controls that have an additive effect is key to informing 'right-sizing' decisions. The latter improves security posture, while the former has a negligible impact on security. As such, when security resources are weighed against implemented security controls, opportunities to optimize costs can be identified without impacting overall security posture.

5. Re-engineer/Re-platform

Most organizations feel overwhelmed by the amount of cybersecurity alerts that existing tools produce. As a result, companies hire more security professionals to "throw at the problem". An alternative to this is re-engineering or re-configuring existing security tools to remove false positives and provide more meaningful alerts. Cost savings can be achieved by reducing the amount of full-time employees, contractors, or Managed Security Service Providers (MSSPs) required to monitor security tools by just re-configuring the tools to be more efficient and effective. Cybersecurity programs can also assess existing processes and interconnections between other teams to uncover areas that can be re-engineered and made more efficient.

Re-engineering security tools usually improves the security posture of an organization to better identify, detect, and respond to potential attacks. Further, re-engineering processes can result in "non-security" processes being offloaded to the responsible teams. As a result, this can reduce overall cybersecurity program spend and will allow security team members to focus on processes that impact the overall security posture of the organization.

6. Automate

The operational duties carried out by security teams can become resource-intensive when the processes are manual and scaled across the size of the organization. For instance, the process of allocating roles and responsibilities to hundreds of thousands of identities requires a significant portion of time. Security functions are also burdened with high volumes of vulnerabilities every week, which require remediation within short timeframes. Manual vulnerability and patch management processes place superfluous strain on stretched security teams, which reduces the likelihood of meeting remediation targets and increases the organizational attack surface.

Automating the manual processes reduces the number of bottlenecks that curtail the overall security posture. The operational efficiency gains typically outweigh the significant upfront investment in time required to configure automated tooling to minimize noise volumes and the training required for users of the tooling.

7. Insource/Outsource

Security teams are often organized in such a manner that staff share overlapping security responsibilities, which can lead to inefficiencies and inhibit the development of the security program. This is compounded when teams form siloed structures with poor communication flows, which yields duplications of effort.

The key to understanding whether to insource or outsource a security capability is to weigh the maturity, size, availability, and technology requirements against the associated costs and timelines. Outsourcing security services provides organizations with quick access to a mature capability that may be otherwise resource-intensive to develop internally. Whereas, insourcing a capability can provide more control and direction over the capability, while providing cost saving opportunities in the long-term.

Getting started: What can you do next?

The seven levers discussed here (simplify, re-negotiate, prioritize, right-size, re-engineer/re-platform, automate, and insource/outsource) provide organizations with a toolkit to enact change. Positive changes to the team can be realized as a result of optimizing cybersecurity costs, such as enhanced collaboration, greater transparency, and stronger relationships with strategic partners.

Knowing where to begin can be challenging since organizations need to take a holistic approach to identify which of the seven levers to exercise. These levers should be balanced against the people, processes, and technology that underpin the security program. The steps you can take to begin the cybersecurity cost optimization journey are as follows:

1. **Conduct an assessment:** Perform a cybersecurity cost optimization assessment that includes the seven levers discussed to uncover areas of improvement and gain insight into how security maturity and security risks may be impacted.

2. **Find the efficiencies and balance:** Review the security program operating model, organizational structure, and service delivery model to identify efficiencies.

3. **Develop a path forward:** Define the security program blueprint for action that details the cost saving initiatives implementation plan.

4. **Implement cost optimization guardrails:** Balance expenditure against the strategic objectives of the security program and maintain costs within the desired bounds.

AlixPartners works with senior leaders across organizations to efficiently identify, quantify, and implement cost optimization opportunities for cybersecurity programs. A QuickStrike assessment of cybersecurity program expenditure is a helpful way for organizations to prepare to minimize spending, maximize efficiency, and extract the most value from security investments. If you would like to discuss our cost optimization QuickStrike assessment, please contact one of our experts below.

26.Biden's Cybersecurity Plan Leaves Quantum Sector Wanting More

by Fierce Electronics
https://www.fierceelectronics.com/electronics/bidens-cybersecurity-plan-leaves-quantum-sector-wanting-more

The New National Cybersecurity Strategy For The U.S., Unveiled Last Week By The Biden Administration, Highlighted The Importance For Federal Government Agencies And The Private Sector To Upgrade Current Encryption To Provide Better Protection Against The Future Security Threats Posed By Quantum Computers. However, Anyone Hoping For New Or More Specific Statements About The Role Quantum-Safe Measures Will Play In The Future Was Left Wanting.

In Recent Weeks, Expectations Had Begun To Build That The Strategy Might Feature New Language And Details About The U.S. Government's Plans To Take A Leadership Role In The Migration To Quantum-Safe Security. Dylan Presman, Director Of Budgets And Assessments For The Office Of The National Cyber Director, Said During A Presentation Hosted Last Month By The Advanced Technology Academic Research Center That The New Strategy Likely Would Feature "A Strong Stand On Quantum Especially On The Transition [To Quantum-Safe Cryptography]."

Meanwhile, news that Chinese researchers had made progress on methods to break current RSA encryption using quantum computing resources that could be available in the near future led some to believe that the new strategy would specifically call out the quantum threat posed by China. (The research claim has since been widely disputed and discredited.)

"I want a little vehemence [in statements from the federal government] to show why this is so important," one source from a quantum technology firm told Fierce Electronics back in January. "The claim is being downplayed, but the quantum race with China is real."

As it turned out, there was a brief quantum-specific section included in the 39-page document that, in the span of two paragraphs, described quantum-safe encryption (sometimes called post-quantum cryptography, or PQC) as a "priority" for the federal government. The strategy document, which carried the signature of President Joe Biden, stated, "We must prioritize and accelerate investments in widespread replacement of hardware, software, and services that can be easily compromised by quantum computers so that information is protected against future attacks."

Beyond that, the strategy offered nothing new on the quantum front, instead referring to how earlier national security memos from the Biden Administration such as NSM 10, issued in May 2022, outline "a process for the timely transition of the country's cryptographic systems to interoperable quantum-resistant cryptography."

While the new strategy mainly reiterated previous statements, should be noted that the federal government has been far from silent over the last year regarding quantum computing and the security threat posed by it. In addition to several statements from the White House during 2022, Congress also last year approved the Quantum Computing Cybersecurity Preparedness Act.

In addition, Presman's February presentation was timed with a release from his office of "guidance and templates to federal departments and agencies for the inventory of cryptographic systems," he said, an important step in preparing for the migration to quantum-safe cryptography. Those agencies now face a

May 4 deadline to submit these inventories and then a June 3 deadline “for submitting cost estimates for the transition to post-quantum cryptography to the administration.” After that, Presman said that by Oct. 18, his office “will issue a report.. on the migration plans for the entire federal federal government, including cost estimates…”

27.Securing Data For A Post-Quantum World

by Brian Bothwell and Marisol Cruz Cain
https://www.gao.gov/products/gao-23-106559

Cryptography uses math to secure or "encrypt" data—helping governments, businesses, and others protect sensitive information. While current encryption methods are nearly impossible for normal computers to break, quantum computers could quickly and easily break certain encryptions and put data at risk.

This spotlight looks at how to better secure data before quantum computers capable of breaking those encryption methods are ready in possibly 10-20 years. Researchers have developed and are standardizing encryption methods capable of withstanding the threat. The longer it takes to implement these new methods, the higher the risk to data security.

Why This Matters

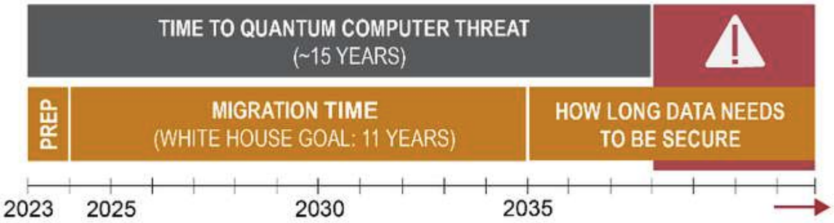
While the emergence of quantum computers offers potential benefits, these computers could undermine the security of current encryption methods that protect sensitive information. If encryption methods able to withstand the capabilities of quantum computing are not developed and deployed soon, secure data could be decrypted as soon as the 2030s.

The Technology

What is it? Quantum computing poses risks to the security of sensitive data, which researchers are working to address. Governments, organizations, and individuals rely on cryptography to keep sensitive and personally identifiable information secure. Cryptography protects information by transforming it using mathematical functions, collectively referred to as encryption. Current, widely used encryption methods rely on complex mathematics that are nearly impossible for normal, or classical, computers to break in reasonable time frames.

Quantum computers, in contrast, could break certain types of widely used encryption methods, such as those used for secure website connections, in exponentially shorter times because of key differences in information processing. As described in an earlier GAO report , classical computers process information through bits that can only be 0 or 1 (like an on/off switch). A quantum computer, however, processes information using quantum bits, or qubits, which can be any combination of 0s and 1s simultaneously due to properties of nature at small scales.

Quantum computers that could break current encryption methods— known as cryptographically relevant quantum computers (CRQCs)—may not exist for another 10 to 20 years, according to some experts. The largest quantum computer currently developed only has a small fraction of the necessary qubits for a CRQC. However, data encrypted with current methods can be downloaded and saved for future decryption by CRQCs. For example, technology designs relevant for long periods are at risk if a bad actor steals them and later decrypts them with a CQRC. In other words, if the migration time plus the time data must be securely retained is longer than the time it takes for CRQC development, then data will be unprotected.

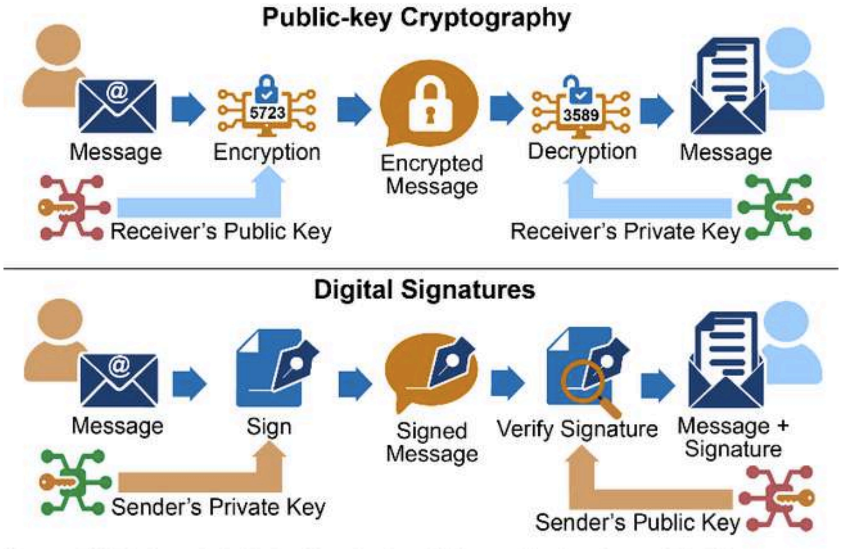


🟥 Data unprotected

Source: GAO adaptation of Mosca's theorem. | GAO-23-106559

To combat the threat of CRQCs, researchers are developing and standardizing new encryption methods collectively referred to as post-quantum cryptography (PQC). These new methods are intended to withstand attacks from both quantum and classical computers.

How does it work? Cryptography protects sensitive data using a series of characters called a "key" which can be public or private. Senders and receivers use keys to lock (encrypt) and unlock (decrypt) the transmitted data. There are three main types of cryptography: private-key, public-key, and digital signatures. Experts generally agree that encryption methods for private-key cryptography are less susceptible to attack by CRQCs and easier to make more secure by using larger key sizes. In contrast, experts generally agree that current encryption methods commonly used for public-key cryptography and digital signatures are susceptible to attack by CRQCs. Public-key cryptography includes the encryption of e-mail and other digital transactions and digital signatures include the virtual signing and authentication of documents.



Source: GAO (adaptation), National Academies of Sciences, Engineering, and Medicine, © *Cryptography and the Intelligence Community: The Future of Encryption*, Figures S.1.2 and S.1.3, 2022, https://doi.org/10.17226/26168 (analysis), icons-studio/stock.adobe.com (images). | GAO-23-106559

The mathematical structure underlying current encryption methods commonly used for public-key cryptography and digital signatures could be broken with a CRQC. For example, the Rivest-Shamir-Adleman

(RSA) algorithm—a widely used public-key encryption method for exchanging of sensitive information, such as bank transfers—would take billions of years for a classical computer to decrypt, but only hours or days for a CRQC.

Options for replacing current public-key encryption methods fall under different families of challenging mathematical problems that should not be susceptible to decryption by classical or quantum computers. Lattice-based encryption, for example, relies on geometry in a highly multidimensional space. This results in a system that should be much more difficult to decrypt, according to experts.

How mature is it? PQC methods have been developed and are undergoing standardization for implementation. A National Institute of Standards and Technology (NIST) public initiative has been developing replacements for at-risk encryption methods since 2016. In July 2022, NIST selected four PQC algorithms the agency will standardize. The National Security Agency plans to incorporate the algorithms into its commercial national security algorithm suite once NIST releases the standards, anticipated in 2024. NIST is also collaborating with expert and standards groups, such as the International Organization for Standardization, which are developing their own PQC standards. Other countries are also working on their own PQC methods.

Why now? While experts do not agree on when a CRQC will be developed, they do agree that the time to prepare for PQC is now. The Office of Management and Budget issued guidance in 2022 on how to identify and prioritize at-risk encryption methods and information for an efficient transition to PQC once the NIST standards are available. For example, sensitive information with long security lifetimes, such as personally identifiable information, would be prioritized in the transition.

Organizations that are unaware of the extent of cryptography use in their systems may need to make unexpected infrastructural changes. For example, PQC may require upgraded microprocessors. Further, in a 2022 national security memorandum, the White House outlined the need for growing an informed PQC workforce in the U.S., as well as the need for ensuring interoperability between federal agencies during the PQC transition. The White House has called for federal agencies to complete the transition to PQC by 2035, but this may not be soon enough to keep data safe from future decryption.

Opportunities

- **Enhanced data security.** Even if a CRQC is never developed, creating more complex encryption methods could make sensitive and personally identifiable information more secure.

- **Modernized infrastructure.** The technology updates needed for transition to PQC may result in modernized infrastructure that is more agile for future updates than systems that have encryption methods incorporated into their hardware.

Challenges

- **Lengthy transition.** Identifying and replacing affected technologies may take a long time, and the longer the transition to PQC takes, the more that sensitive information will be at risk.

- **Cost and complexity.** Transitioning to infrastructure supportive of new encryption methods will be expensive and complex. Organizations may face challenges in planning for incurred costs and in remaining operational during the infrastructure changeover.

- **Workforce gaps.** The U.S. requires more data security and quantum computing expertise than is currently available. For example, one study predicts that fewer than 50 percent of quantum computing jobs may be filled by 2025.

- **Information sharing.** As organizations adopt PQC, some—such as those in law enforcement and national security—may hesitate to share information with those that have not transitioned to PQC.

Policy Context and Questions

- What additional steps could policymakers take to protect against decryption of sensitive data by quantum computers?
- What additional planning may be needed to upgrade infrastructure to support PQC?
- What actions could help build a workforce capable of understanding, implementing, and advancing PQC as needed?

28.A Key Post-Quantum Algorithm May Be Vulnerable To Side-Channel Attacks

by Daryna Antoniuk
https://therecord.media/a-key-post-quantum-algorithm-may-be-vulnerable-to-side-channel-attacks

As companies and governments around the world work on creating usable quantum computers, security researchers are also devising ways to protect data once those machines are available.

Quantum computers have the potential to crack the cryptographic algorithms in use today, which is why "post-quantum" cryptographic algorithms are designed to be so strong that they can survive huge leaps in computing power.

A team in Sweden, however, says it's possible to attack some of the new algorithms with other methods.

Researchers at the KTH Royal Institute say they found a vulnerability in a specific implementation of CRYSTALS-Kyber — a "quantum safe" algorithm that the U.S. National Institute of Standards and Technology has selected as part of its potential standards for future cryptographic systems.

According to the Swedish team, CRYSTALS-Kyber is vulnerable to side-channel attacks, which use information leaked by a computer system to gain unauthorized access or extract sensitive information. Instead of trying to guess a secret key, a side-channel technique analyzes data such as small variations in power consumption or electromagnetic radiation to reconstruct what the machine is doing and find clues that would enable access.

CRYSTALS-Kyber was designed to be resistant to side-channel attacks, but the researchers said they had success using machine learning as part of their experiment, calling it a "breakthrough" in testing quantum-safe technology.

Machine learning "can overcome conventional countermeasures," such as "masking," which involves hiding the secret key using random numbers. Even if someone observes the encryption process, they can't discover the key.

Previous research on CRYSTALS-Kyber analyzed the algorithm with up to three "orders" of masking, but the Swedish team said it demonstrated its technique on fifth-order masking.

“The presented approach is not specific for CRYSTALS-Kyber and can potentially be applied to other schemes,” the researchers said.

New approach

The machine learning in the side-channel attack involved a neural network training method called recursive learning. This method made it possible to extract the smallest data units with high probability, the researchers said.

“This is a very notable, and novel, aspect of the research,” said Lukasz Olejnik, an independent cybersecurity researcher and consultant who did not participate in the study.

According to him, machine learning can be used to efficiently analyze data and learn patterns that reveal security weaknesses of the system. The researchers also said they could use machine learning to test algorithms for resistance to other types of attacks.

The attack targeted the specific implementation of CRYSTALS-Kyber, not its principles. A specific implementation of a post-quantum algorithm refers to its practical application in a software or hardware system.

“As long as the core principles stand and remain robust, we'll live with those,” Olejnik said.

A NIST official, Dustin Moody, told SC Magazine that this distinction is important, because the Swedish research “breaks a particular implementation that they’re working with, but it didn’t break the algorithm in general.” NIST is sticking with CRYSTALS-Kyber for its program, he said.

The agency did not respond to The Record’s request for comment.

According to Olejnik, it is necessary to research such attacks because they help create secure methods for implementing, deploying and utilizing the new cryptosystems.

CRYSTALS-Kyber is the only general-purpose algorithm selected so far for the NIST program. Three others are used for digital signature and identity verification.

Researchers need several post-quantum algorithms because it is currently unclear which ones will be most effective and secure against quantum computers.

29.Securing IoT Devices With Lightweight Cryptography

by Bart Stevens
https://semiengineering.com/securing-iot-devices-with-lightweight-cryptography/

The National Institute of Standards and Technology (NIST) recently announced the selection of a new family of cryptographic algorithms called ASCON, which have been developed for lightweight cryptography applications. In this blog, we will explore what lightweight cryptography is and why it is worth considering for specific Internet of Things (IoT) use cases.

In summary, lightweight cryptography aims to make symmetric cryptography as small and energy efficient as possible, while maintaining sufficient security so that short-lived or low-cost devices can still be operated securely. Think of it this way: does an IoT lightbulb require security comparable to AES-256 to be turned on or off? Does an RFID card that has a lifetime measured in a few years, and is used for cafeteria payments, require security against quantum computer attacks? They of course need robust security, just not at the same level as some applications require.

The common consensus is that 128-bit is an acceptable security level for most use cases: secure against classical computers for the foreseeable future, but not secure enough to be considered post-quantum secure. This is what NIST chose as the targeted security level for their Lightweight Cryptography standardization effort. But why is a new algorithm needed? After all, AES-128, SHA-256 and SHA3-256 all address this security level and are very widely deployed and supported.

Anyone looking at infrastructure installation will know how important interoperability concerns are. But when it comes to IoT, there are enough devices where every gate saved on a chip helps to make the product viable and where every nano Joule saved extends precious battery lifetime. Compared to supporting AES-128 on those devices, it is often much easier to add an additional algorithm to the aggregator chip that collects data from multiple IoT devices and communicates with the backend servers.

If DPA countermeasures need to be considered, this is even more true. Neither AES-128 nor HMAC-SHA2-256 are particularly easy to protect against DPA attacks. The scientific community has made great gains in designing DPA-friendly symmetric algorithms since AES and SHA-2 were developed. NIST has recognized this, and the lightweight cryptography competition, in which ASCON was selected to become the standard, was designed to find an algorithm that provides both AEAD (Authenticated Encryption with Additional Data) and hash functionality at optimal cost, not just in software and hardware implementations, but also when DPA countermeasures are required. For a detailed look at the ASCON algorithm, download our recent white paper Lightweight Cryptography: An Introduction.

As we have seen, lightweight cryptography can be a valuable tool for providing security in area and power constrained IoT devices. As a leading provider of cryptographic IP cores, Rambus can support customers implementing the ASCON algorithms with the ASCON-IP-41 Crypto Engine IP core. The ASCON-IP-41 Crypto Engine supports the two primary algorithms proposed under the ASCON family: ASCON-128/HASH and ASCON-128A/HASHA, for both authenticated encryption with AEAD and HASH modes of operation. To learn how the engine works and learn about potential use cases, visit the Rambus website.

30.Assume The Superposition: Intel Emits SDK To Simulate Quantum Computers

by Tobias Mann
https://www.theregister.com/2023/03/01/intel_quantum_sdk/

Intel has released a Quantum software development kit (SDK) that simulates a complete quantum computer using conventional hardware.

Chipzilla's released the kit in recognition of the fact that the few working quantum systems from the likes of IBM or D-Wave, are prohibitively expensive to buy or rent for early quantum experiments.

The silicon slugger therefore hopes the SDK allows developers to start experimenting with quantum algorithms and how they can be integrated into existing platforms, with an emulator.

"It will not only help developers learn how to create quantum algorithms and applications in simulation, but it will also advance the industry by creating a community of developers that will accelerate the development of applications," Anne Matsuura, director of Quantum applications and architecture at Intel Labs, explained in a statement.

Proponents of quantum computing believe the technology will deliver machines so powerful they'll make classical computers look like slide rules, allowing scientists to swiftly make breakthroughs in fields such as encryption, real-time pathfinding, and drug discovery.

While that sounds lovely, existing quantum computers are hard to build, harder to operate, and even the most advanced quantum systems – IBM's Osprey, for example – might have a few hundred qubits, well short of the hundreds of thousands of logical qubits required to achieve the promised revolution.

Another challenge – which Intel's SDK seems to target – is finding practical applications for quantum computers. Any hardware is only desirable if there's software to run on it, and at present humanity's knowledge of what works well on a quantum machine is limited, hype about drug discovery and all that notwithstanding.

Intel claims its Quantum SDK allows developers to get a head start by letting them build software while engineers figure out how to put actual qubits into working and accessible quantum computers.

The SDK is written in C++ using a low-level virtual machine compiler, which the company says makes it easier for developers to simulate quantum environments and integrate them into their existing C, C++, and Python applications.

Intel's Quantum Simulator (IQS) – an open source project that's been kicking around for a few years now – provides a backend for the SDK. IQS simulates generic qubits, which in theory should allow developers to port their work to real quantum systems in the future.

If any of this sounds familiar, it's because Intel isn't the only company trying to emulate quantum systems using conventional platforms. Last year, Fujitsu claimed it had develop the world's fastest quantum simulator, capable of handling 36 qubit quantum circuits.

However, as anyone who's dabbled with hardware emulation will know, simulating logic in software can be incredibly inefficient. This certainly was the case for Fujitsu's simulator, which required a 64-node cluster of its PRIMEHPC FX 700 boxes, each powered by the Arm-based A64FX processor at the heart of the Fugaku supercomputer.

By comparison, Intel's IQS supports simulations up to 32 qubits on a single node – or can be scaled out to multiple nodes to emulate larger systems. The SDK will eventually work with Intel's own quantum hardware, including the Horse Ridge II control chip and upcoming quantum spin qubit chip.

Intel admits there's still work to be done to fully integrate the SDK with its quantum hardware – assuming that CEO Pat Gelsinger doesn't take the ax to the project as he attempts to turn around Chipzilla's wonky finances.