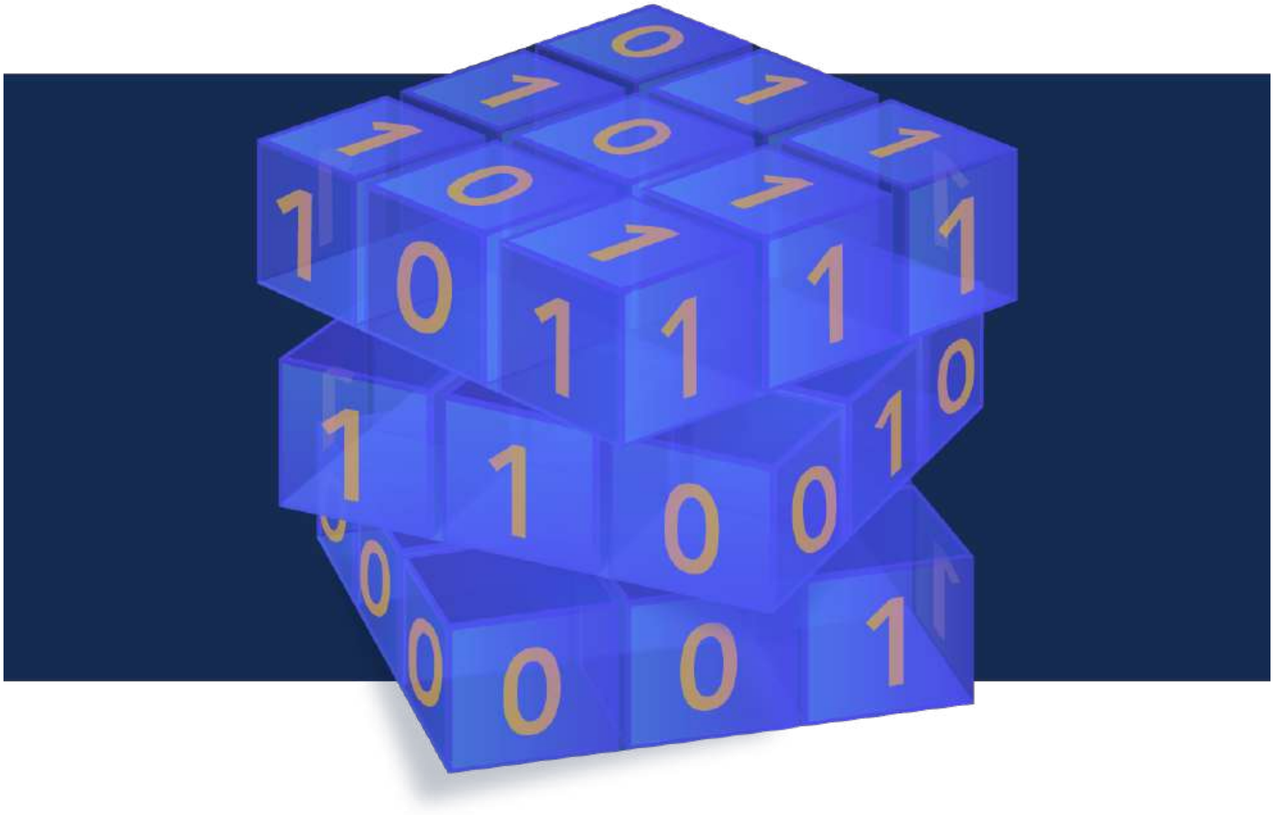
Crypto News

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

January 01, 2023



TABLES OF CONTENTS

Editorial

Happy New Year! Hopefully you were able to take a well-deserved break before getting back to it in 2023. What better way to start the year than to expand your technical knowledge. As we all know, technology doesn't sleep so it's time to catch up on all things quantum, cybersecurity, and technology in this month's issue of Crypto News!

Let's start with article 4 which has promising information about a universal quantum computer which will have more than 1,000 qubits. More specifically, keep an eye out for IBMs Condor processor which is set to be released this year. It will have 1,121 qubits and will be the first of its kind in the world. Other companies have built quantum computers with up to 5,000 qubits but those were for a specific problem while IBMs is universal. Navigate over to the article for more information about what IBM has planned for 2023 as well as the coming years.

Next, take a few minutes to read article 20 which brings to the forefront the classic discussion of user privacy vs. security. Oftentimes, the "security" being referred to is cybersecurity but in this case it's national security. Apple has announced their plan to roll out "end-to-end and user-only-access encryption" to iCloud accounts. The big concern for this proposed upgrade is coming from the FBI in the United States of America. Why? As you may have correctly guessed, it's the loss of their ability to access photos, messages, and other data stored by criminals, bad actors, and other threats to national security. Sounds like a valid concern to me and one that warrants a deeper discussion. So readers, what do you think? What's more important to you personally? User privacy or national security? How about as a technology professional?

As always, I wasn't able to highlight all of the fantastic articles in this issue of Crypto News and I'm confident that more than one article will catch your eye as you thumb through. Let me know what you found interesting and let's discuss!

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

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

1.Counting Down To Quantum? Here's What Security Teams Need To Know

by Greg Wetmore
https://www.cpomagazine.com/cyber-security/counting-down-to-quantum-heres-what-security-teams-need-to-know/

The post-quantum world is often described as a doomsday scenario. One of the biggest fears about quantum computing is its ability to break the traditional encryption algorithms that have protected our data for decades. In response to this pending crisis, President Joe Biden signed two quantum computing presidential directives in 2022, signaling the time is now to figure out how to handle the emerging technology. If you are thinking about how to incorporate post-quantum security readiness into your IT strategy, consider this expert advice.

In this interview, Greg Wetmore, VP Software Product Development and Entrust Cybersecurity Institute member, shares what IT security teams need to know as they prepare for the post-quantum threats on the horizon.

Can you briefly explain what post-quantum cryptography is and how organizations can prepare for it? What steps must organizations take to properly defend themselves in a post-quantum world?

Post-quantum cryptography is a set of cryptographic systems that can protect data from attacks launched from either quantum computers or today's classical computers. After a mathematician named Peter Shor demonstrated that a quantum computer could easily break the algorithm used for public key encryption (PKE), cryptographers around the world began to explore what a post-quantum cryptography system would look like.

Modern public key cryptography uses two common algorithms (RSA and Elliptic Curve) that scramble data into codes only reversible by the holder of the private key; however, quantum computers can reverse engineer this scrambled data without needing the keys. Quantum computers are steadily approaching the computing power and stability they'll need to break the public key encryption protocols widely used in digital systems today to protect sensitive data, applications, and transactions. As a result, organizations must begin moving to quantum-resistant cryptography to protect mission-critical data.

Here's a roadmap for infosec teams looking to get a head start on post-quantum migration:

- **Inventory data:** Map out where your most sensitive and long-life data resides.
- **Inventory cryptographic assets:** Gain in-depth visibility into what cryptographic assets already exist in your environment.
- **Build a cryptographic agility strategy:** Cryptographic agility will be critical for the PQ transition. Crypto agility is the ability to easily move from one algorithm to another – even a quantum-resistant one.
- **Test and plan the migration:** The technology behind quantum-safe cryptography is rapidly advancing. The NIST PQ Competition recently announced the 4 algorithms that will be standardized over the next year. Some security vendors are beginning to offer early access to quantum-safe

crypto in their products.

When should organizations begin preparing for a post-quantum future? And how can IT security teams determine whether it's urgent to act or not?

Quantum computing is advancing, and while experts are not sure when there will be a quantum computer powerful enough to break the RSA and ECC cryptographic algorithms that are currently in use, many are operating under the assumption that this can happen within a 10- to 15-year timeframe.

Last month, the NSA released the Commercial National Security Algorithm Suite 2.0 to provide timing parameters for specific areas and industries to migrate to quantum-resistant cryptography. They identified the first area to be addressed is software and firmware signing, and that transition should begin immediately.

The migration to quantum-safe algorithms could take several years, and for some industries – like healthcare and financial services – the transition is already underway due to technology lifecycles and long-life data that has to remain secure. To put it into perspective, the migration from SHA-1 to SHA-2 raised numerous alarm bells for the security and cryptography community and it was generally seen as a straightforward migration. But when the time came, organizations struggled with it and some are still figuring it out today. The transition to post-quantum will be more complex than cryptographic transitions in the past. This should be a call to action for organizations to begin considering the impacts to their digital infrastructure.

What are some of the most common threats associated with post-quantum computing?

Quantum computing promises to solve difficult problems — and create entirely new ones.

Quantum computers use the laws of quantum mechanics to process information in quantum bits, or qubits. A system built on qubits can exist in multiple states at the same time (called quantum superposition). This amazing property allows quantum computers to process data and solve some kinds of problems at an exponentially faster rate than classical computers. It has been proven that a scaled quantum computer will render modern public-key encryption algorithms useless. With many enterprise technologies currently dependent on public-key encryption, they're placed at an elevated risk of brute-force attacks by malicious actors.

Keeping in mind the vast speed by which quantum computers can operate, we humans must begin the long migration to post-quantum readiness. It's likely that adversaries are already harvesting encrypted data and storing it until quantum computers have enough qubits to crack the encryption algorithms. Don't underestimate the effort needed to migrate to post-quantum cryptography – the effort will take years.

What types of software updates or security upgrades will be required to defend against the quantum threat? And how long could these take?

Software updates will be significant, and doing so securely will become a problem in and of itself. Think about large organizations with data centers and edge devices scattered across the globe. These updates will take time and require a carefully planned strategy, inventorying and expertise to be developed well in advance. Migrating to a cloud infrastructure offers some advantage but those still with a lot of physical machines and hardware will need time for updates; some machines might even be incapable of receiving updates and would have to be replaced – a situation that can be costly and time-consuming.

Now that we've discussed the bad. Can you give us a cool takeaway on quantum computers? Anything to get excited about?

Despite their impact on cybersecurity, quantum computers can offer a lot of benefits and solve a wide range of problems facing humanity. One area, in particular, is medicine and biopharma. We expect quantum computers to enhance our ability of drug discovery and development, and allow scientists to conduct new research for the benefit of raising efficacy and access. Quantum simulations could also play a role in developing the vaccines of the future to protect against widespread viruses and disease.

These simulations could also be unleashed for the benefit of conservation and environmental initiatives. Scientists predict these simulations could lead the way to new scientific breakthroughs and drastically enhance our ability to recycle carbon dioxide and other fuels essential to keeping society moving.

Overall, the ability of quantum computers to more efficiently perform calculations that model real physical systems with huge data sets will make them invaluable to many industries like: materials science, weather forecasts, natural language processing, financial modeling and more. However, if security teams are unable to secure their environments, then much of our everyday web interactions will be at risk. Take the proper steps now to avoid panic later on.

2.The Future Is Quantum – How Organisations Can Prepare Themselves

by James Cook
https://www.cpomagazine.com/cyber-security/the-future-is-quantum-how-organisations-can-prepare-themselves/

Faster development of vaccines and green battery technology, as well as deeper analytics and faster trading in the financial markets – these are just some of the benefits that countries in APAC are looking to achieve as they adopt quantum computing. In China, the government has allocated US$10 billion to the construction of the National Laboratory for Quantum Information Sciences in 2020. In Singapore, they have launched the National Quantum Computing Hub and the National Quantum Safe-Network. The acceleration in quantum computing has made leaps and bounds, and businesses are already anticipating the future of quantum.

While quantum computing will bring about massive changes and value across various industries, it also introduces new and much more dangerous threats. Quantum computing could drastically cut down the time needed to crack the strong cryptographic algorithms we rely on today – potentially from decades to minutes.

Although cyber security leaders might think they have time to prepare, the post-quantum era has already begun – and many companies are currently ill-equipped to handle such development.

In a study by (ISC)², the global cyber security workforce needs to grow by 65% to effectively prepare and defend against cyber threats. It is proving difficult for security teams to handle day-to-day cyber threats, let alone prepare for those powered by quantum technology. The same study also highlights that this is particularly dire within the APAC region, which has a cyber security workforce gap of 1.42 million. There is an urgent need for organisations to prepare themselves for the quantum computing era – and the sooner they start, the better.

The need to adapt and achieve crypto agility

Advances in quantum computing threaten the integrity of traditional asymmetric encryption algorithms.

Protocols like the RSA algorithm, Elliptic Curve Cryptography, and Finite Field Cryptography will no longer be able to defend against such brute force attacks. Organisations will need to adopt other methods to ensure their data is safe.

Migrating to quantum resistant algorithms will take years to integrate into existing systems and processes. To make matters worse, adversaries already have a head-start. Many have begun collecting and storing encrypted data, waiting for quantum computers to gain sufficient strength to break through the algorithms before launching their attacks.

Organisations, therefore, need to achieve crypto-agility – the ability to change, improve, and revoke cryptographic assets to successfully deal with such threats.

Not too late to prepare for the post-quantum era

There are four steps organisations need to take to attain crypto agility:

- Take inventory
- Prioritise data
- Test
- Plan

Firstly, companies need to know what cryptographic assets and algorithms they possess, as well as the places they reside and what they're used for. A comprehensive view of all data and keys will minimise margins for error, allowing for more efficient and effective decision making.

Secondly, once companies know what and where their data is, they need to prioritise them. By categorising data according to their value and risk level, organisations can decide which needs to be migrated to post-quantum cryptography first.

Thirdly, organisations need to start prototyping. The National Institute of Standards and Technology (NIST) has selected four quantum-resistant cryptographic algorithms that companies can use to test their data security and prepare for forthcoming threats.

Lastly, companies need to develop a post-quantum cryptography strategy and involve their vendors in the process. With a structured plan detailing the process of migration, organisations will be ready to take on post-quantum cryptography and assimilate into the new technological era.

As we move towards the quantum age, organisations will inevitably face challenges in upholding their security standards. What's more, cyber criminals have already started making their moves to take advantage of their instability during this transition period.

The time to start migrating to post-quantum cryptography is now. Organisations, therefore, need to work with trusted vendors who can help them achieve crypto-agility and smoothly adjust to this new era of technology and threats.

3.One Step Closer To Securing Our Nation From The Quantum Threat

by Skip Sanzeri

https://www.forbes.com/sites/forbestechcouncil/2022/12/27/one-step-closer-to-securing-our-nation-from-the-quantum-threat/?sh=226358f5429f

Every day, each one of us increases our digital footprint by generating volumes of data collected through our use of computers and mobile phones. Used Waze lately? Ordered anything on Amazon? Logged onto or visited *any* websites? If you think about it, most of our decisions, behaviors, preferences and locations are now stored in vast databases that are accessible via the internet to adversarial nation-states and nefarious individuals.

Decades ago, we could not have imagined how much information we would create and then willingly trade for convenience. Today, with every click, swipe or audible word, we are continually adding to the mountain of data and personal information already stored electronically. To make things worse, the future will offer us unrefusable deals to create even larger digital shadows for machine learning and (eventually) AI to process.

According to Statista, the amount of data created and captured globally could reach 120 zettabytes in 2023 (each zettabyte is 1 billion terabytes). Up to 2025, global data creation is projected to grow to more than 180 zettabytes. Unfortunately, due to our use of the internet, all this data can be accessible to hackers, thieves and those who would disrupt or cause harm. In other words, there is no future scenario that offers less risk of our data and systems being compromised.

A New Threat

To date, the encryption we use to protect our data and communications (encryption is the technology that is designed to keep our data safe as it travels through networks and over the internet and while it is stored) has held up to a great extent. Since this encryption was designed to thwart data decryption by the types of computers we use today, it's done a reasonable job of protecting us from theft and harm.

However, now we have a new threat to worry about. Quantum computers are very powerful machines that, due to the way they process data, have been proven mathematically via an algorithm designed by Peter Shor (called "Shor's Algorithm") that they will crack the current encryption we all use globally to access the internet.

We know that nation-states are spending tens of billions on quantum computers that can decrypt data already stolen, which poses a threat to our way of life (think banking, healthcare, military and government secrets). If an adversarial nation-state brings a powerful quantum computer online before we can protect our data and communications, we will have an unmitigated disaster on our hands. Worse yet, data stolen today will be decrypted in the future by a quantum computer. And if that data needs to stay private for decades (e.g., financial information for 25 years; national and military secrets for 50 years; healthcare data for 75 years), then much of the data remains valuable when a quantum computer is available to decrypt it.

Our U.S. Government To The Rescue

The good news is that our nation is responding. On November 18, the Office of Management and Budget published a mandate for our federal government to start an upgrade to quantum-safe cryptography (this is software that can withstand a quantum computing attack). The memo (M-23-02) requires that federal agencies comply with the National Security Memorandum 10 (NSM 10) from May 2022, which is designed to promote U.S. leadership in quantum computing while mitigating risks to cryptographic systems. The memo asks that federal agencies prepare immediately for the threat posed by a cryptographically relevant quantum computer (CRQC).

Also, M-23-02 highlights for federal agency leaders (as mentioned above) that data can be stolen today and decrypted in the future. Anything stolen today could provide an adversary with the ability to steal assets and intellectual property, as well as disrupt (think elections) or cause great harm (energy grids, GPS systems) in the future.

So, M-23-02 is mandating federal agencies to start the upgrade process now to secure their data so that even if it is stolen, it has quantum protection, which means it could remain encrypted and non-accessible for decades. OMB has set a deadline for all federal agencies to submit their CRQC vulnerability inventories by May 4, 2023—and annually until 2035, focusing on high-value assets and high-impact systems. Each agency must identify a migration lead and submit them to OMB within 30 days of the memo or by December 18, 2022.

Make no mistake: Quantum computers pose an existential risk to our way of life in the U.S. According to Arthur Herman, a Forbes contributor and senior fellow and director of the Quantum Alliance Initiative at Hudson Institute, a single quantum attack on our banking system could cause nearly $2 trillion in damage. A foreign nation-state with a CRQC would have global domination potential at its fingertips.

The OMB's directive has put in place a process for federal agencies to prepare well ahead of time, recognizing the importance of post-quantum security measures. Countries and organizations worldwide should track this effort so they, too, can start preparing for a future where quantum computing is commonplace.

4.An IBM Quantum Computer Will Soon Pass The 1,000-Qubit Mark

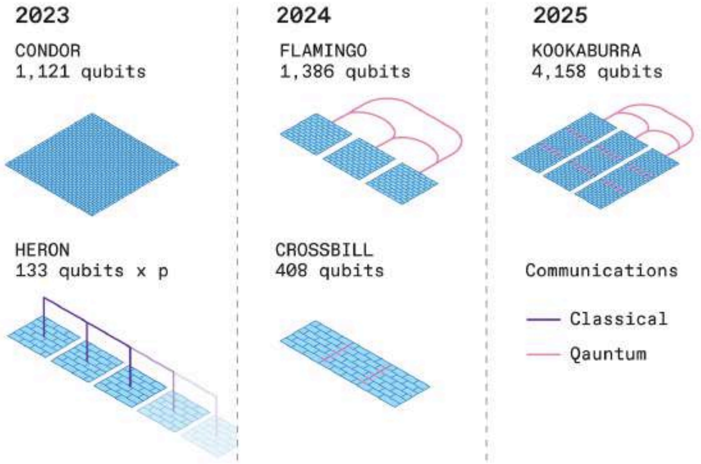
by Charles Q. Choi
https://spectrum-ieee-org.cdn.ampproject.org/c/s/spectrum.ieee.org/amp/ibm-condor-2658839657

IBM's Condor, the world's first universal quantum computer with more than 1,000 qubits, is set to debut in 2023. The year is also expected to see IBM launch **Heron,** the first of a new flock of modular quantum processors that the company says may help it produce quantum computers with more than 4,000 qubits by 2025.

While quantum computers can, in theory, quickly find answers to problems that classical computers would take eons to solve, today's quantum hardware is still short on qubits, limiting its usefulness. Entanglement and other quantum states necessary for quantum computation are infamously fragile, being susceptible to heat and other disturbances, which makes scaling up the number of qubits a huge technical challenge.

Nevertheless, IBM has steadily increased its qubit numbers. In 2016, it put the first quantum computer in the cloud anyone to experiment with—a device with 5 qubits, each a superconducting circuit cooled to near absolute zero. In 2019, the company created the 27-qubit Falcon; in 2020, the 65-qubit Hummingbird; in 2021, the 127-qubit Eagle, the first quantum processor with more than 100 qubits; and in 2022, the 433-qubit Osprey.

Other quantum computers have more qubits than does IBM's 1,121-qubit Condor processor—for instance, D-Wave Systems unveiled a 5,000-qubit system in 2020. But D-Wave's computers are specialized machines for solving optimization problems, whereas Condor will be the world's largest general-purpose quantum processor.



IBM expects to build quantum computers of increasing complexity over the next few years, starting with those that use the Condor processor or multiple Heron processors in parallel.

“A thousand qubits really pushes the envelope in terms of what we can really integrate,” says Jerry Chow, IBM’s director of quantum infrastructure. By separating the wires and other components needed for readout and control onto their own layers, a strategy that began with Eagle, the researchers say they can better protect qubits from disruption and incorporate larger numbers of them. “As we scale upwards, we’re learning design rules like ‘This can go over this; this can’t go over this; this space can be used for this task,’” Chow says.

With only 133 qubits, Heron, the other quantum processor IBM plans for 2023, may seem modest compared with Condor. But IBM says its upgraded architecture and modular design herald a new strategy for developing powerful quantum computers. Whereas Condor uses a fixed-coupling architecture to connect its qubits, Heron will use a tunable-coupling architecture, which adds Josephson junctions between the superconducting loops that carry the qubits. This strategy reduces crosstalk between qubits, boosting processing speed and reducing errors. (Google is already using such an architecture with its 53-qubit Sycamore processor.)

In addition, Heron processors are designed for real-time classical communication with one another. The classical nature of these links means their qubits cannot entangle across Heron chips for the kind of boosts in computing power for which quantum processors are known. Still, these classical links enable “circuit knitting” techniques in which quantum computers can get assistance from classical computers.

For example, using a technique known as “entanglement forging,” IBM researchers found they could simulate quantum systems such as molecules using only half as many qubits as is typically needed. This approach divides a quantum system into two halves, models each half separately on a quantum computer, and then uses classical computing to calculate the entanglement between both halves and knit the models together.

While these classical links between processors are helpful, IBM intends eventually to replace them. In 2024, the company aims to launch Crossbill, a 408-qubit processor made from three microchips coupled together by short-range quantum communication links, and Flamingo, a 462-qubit module it plans on uniting by roughly 1-meter-long quantum communication links into a 1,386-qubit system. If these experiments in connectivity succeed, IBM aims to unveil its 1,386-qubit Kookaburra module in 2025, with short- and long-range quantum communication links combining three such modules into a 4,158-qubit system.

IBM's methodical strategy of "aiming at step-by-step improvements is very reasonable, and it will likely lead to success over the long term," says Franco Nori, chief scientist at the Theoretical Quantum Physics Laboratory at the Riken research institute in Japan.

IBM's quantum leaps in software

In 2023, IBM also plans to improve its core software to help developers use quantum and classical computing in unison over the cloud. "We're laying the groundwork for what a quantum-centric supercomputer looks like," Chow says. "We don't see quantum processors as fully integrated but as loosely aggregated." This kind of framework will grant the flexibility needed to accommodate the constant upgrades that quantum hardware and software will likely experience, he explains.

In 2023, IBM plans to begin prototyping quantum software applications. By 2025, the company expects to introduce such applications in machine learning, optimization problems, the natural sciences, and beyond.

Researchers hope ultimately to use quantum error correction to compensate for the mistakes quantum processors are prone to make. These schemes spread quantum data across redundant qubits, requiring multiple physical qubits for each single useful logical qubit. Instead, IBM plans to incorporate error-mitigation schemes into its platform starting in 2024, to prevent these mistakes in the first place. But even if wrangling errors ends up demanding many more qubits, IBM should be in a good position with the likes of its 1,121-qubit Condor.

5.Telecom Industry Looks To Quantum Computing To Overcome 5G, 6G Bottlenecks

by Ma Si
http://global.chinadaily.com.cn/a/202212/22/WS63a39277a31057c47eba58d2.html

China Mobile, the world's largest telecom carrier with 900 million mobile subscribers, is exploring ways to tap into quantum computing to overcome computational bottlenecks facing 5G and 6G technologies.

The research institute of China Mobile has signed a deal with Origin Quantum, a Chinese startup focusing on quantum computing.

"This is the first cross-sector cooperation between quantum computing and the telecom industry in China, which has big value in exploring potential applications of quantum computing in big data as well as complex network construction and optimization in the field of mobile communication," said Guo Guoping, a professor of quantum computing at the University of Science and Technology of China and chief scientist at Origin Quantum.

Under the agreement, Origin Quantum, based in Hefei, Anhui province, will provide quantum communication algorithms based on verifications by its superconducting quantum computer, OriginQ Wuyuan, to help overcome the computational bottlenecks facing 5G and 6G.

Cui Chunfeng, president of the future research institute of the China Mobile Research Institute, said the

5G era has seen exponential growth in computing demand from signal processing, network optimization, big data analysis, image processing and other tasks. Traditional computer algorithms are finding it increasingly difficult to meet such demand.

In the future, 6G will require even higher computing capabilities than 5G. It will be necessary to introduce new technologies, such as quantum computing, to help solve this challenge, Cui said.

Quantum computing is widely regarded as one of the most pioneering technologies, given its ability to harness the laws of quantum mechanics and solve calculations too complex for even the most powerful conventional supercomputers.

It would take a quantum computer only 200 seconds to process calculations that the fastest supercomputer would take about 10,000 years to complete, said Dou Menghan, deputy director of the Anhui Quantum Computing Engineering Research Center.

Dou said comparing the computing power of a quantum computer with a conventional computer is like comparing a conventional computer with an abacus.

Cui, from China Mobile, said, "We hope to explore the possibility of applying quantum computing to enable network optimization, network autonomy, network security and the metaverse, and we hope to solve the (computational) bottlenecks for the development of a future network."

Established in 2017, Origin Quantum is ranked first in China and sixth in the world by the number of invention patents it has applied for in quantum computing, according to the latest Global Quantum Computing Technology Patent Filings Ranking List released by the innovation index researcher incoPat and intellectual property media IPR Daily in October.

Han Jian, head of the secretariat of the quantum computing committee of the China Institute of Communications, said China has more than 1.3 billion phone users, and leveraging quantum computing to process telecom data is a new field that could grow into a multibillion-dollar market.

Quantum computing will have a conservative estimated value of up to $700 billion by 2035 for industries such as pharmaceuticals, chemicals, automotive and finance, according to a report by global consulting firm McKinsey& Co.

China said in its 14th Five-Year Plan (2021-25) that it will speed up frontier science and technological blueprints, such as quantum computing and quantum communication.

Internationally, US tech companies such as Google, IBM and Microsoft are accelerating steps to develop quantum computing platforms. Chinese tech heavyweights including Alibaba, Baidu and Tencent have also tapped into the quantum computing sector.

6.Top Quantum Research Stories Of 2022

by Matt Swayne
https://thequantuminsider.com/2022/12/21/top-quantum-research-stories-of-2022/

Research is the fuel for the deep tech industry in general and for the quantum technology industry, specifically.

The industry, itself, is built on theoretical and experimental work that stretches back about a century. But more work is need to make quantum technology practical and ubiquitous.

In 2022, scientists have made significant steps in that direction. Like a reverse game of Jenga, where the players must carefully insert blocks to build and firm up a tall, teetering monstrosity of a building, researchers have made progress in the keystones of practical quantum technology, such as error correction, coherency and quantum volume.

This is a list of just some of these advance, based, in part, on social media, web statistics and acclaim across the media.

Also note in this list the presence of many academic-business partnerships. Quantum startups and quantum divisions in major global corporations, all steeped in science, are partnering with some of the world's most advanced research institutions. It cannot be emphasized enough that these collaborations are, first, vital to the success of the quantum industry. Second, the number of these cross-discipline, cross-industry collaborations show that quantum tech workers can make these complex partnerships with ease, a good sign for eventual success of what might be the world's most exciting and complication computational challenge.

FOUR QUANTUM PIONEERS SHARE THE BREAKTHROUGH PRIZE IN FUNDAMENTAL PHYSICS

Four pioneers in the field of quantum information were among the list of the 2023 Breakthrough Prize laureates, according to a statement from the Breakthrough Prize Foundation. David Deutsch, Peter Shor, Charles H. Bennett and Gilles Brassard were listed as this year's winner in the fundamental physics category. Each winner will receive about $3 million.

IBM UNVEILS 400 QUBIT-PLUS QUANTUM PROCESSOR AND NEXT-GENERATION IBM QUANTUM SYSTEM TWO

IBM announced new advances in quantum hardware and software and outlining its pioneering vision for quantum-centric supercomputing at the annual IBM Quantum Summit. Dr. Darío Gil, Senior Vice President, IBM and Director of Research, told summit attendees that the new 433 qubit 'Osprey' processor will bring the community a step closer to the point where quantum computers will be used to tackle previously unsolvable problems.

PHYSICISTS USE QUANTUM COMPUTER TO PROBE WORMHOLE DYNAMICS

Scientists have, for the first time, developed a quantum experiment that allows them to study the dynamics, or behavior, of a special kind of theoretical wormhole. The experiment has not created an actual wormhole (a rupture in space and time), rather it allows researchers to probe connections between theoretical wormholes and quantum physics, a prediction of so-called quantum gravity.

"This Work Constitutes A Step Toward A Larger Program Of Testing Quantum Gravity Physics Using A Quantum Computer. It Does Not Substitute For Direct Probes Of Quantum Gravity In The Same Way As Other Planned Experiments That Might Probe Quantum Gravity Effects In The Future Using Quantum Sensing, But It Does Offer A Powerful Testbed To Exercise Ideas Of Quantum Gravity." — Maria Spiropulu, The Shang-Yi Ch'en Professor Of Physics, Caltech

RECORD MEASUREMENT BRINGS MASS PRODUCTION OF QUANTUM CHIPS CLOSER

Quantum Motion reportedly achieved a record measurement of quantum devices made on a silicon chip. The company was been able to place thousands of quantum dot devices, integrated alongside control electronics operating at temperatures less than one tenth of a degree above absolute zero, and all realized on a single silicon chip fabricated in a commercial semiconductor foundry. They report this advance lays the foundations for mass production of quantum chips.

RIVERLANE: QUANTUM COMPUTERS MIGHT SHORTEN DRUG SIMULATION TIME

Riverlane-led researchers published a paper in the Journal of Chemical Theory and Computation outlining advances in quantum algorithms that can reduce the amount of resources required for researchers to achieve useful results. Focusing on the cancer growth inhibitor Ibrutinib, the Riverlane team's estimates show that the resources required to run calculations in active spaces of 50 orbitals and electrons, has fallen from over 1,000 years to just a few days.

RECORD MEASUREMENT BRINGS MASS PRODUCTION OF QUANTUM CHIPS CLOSER

Quantum Motion, a UK-based quantum computing start-up led by academics from UCL and Oxford University, achieved a record measurement of quantum devices made on a silicon chip. The company was able to place thousands of quantum dot devices, integrated alongside control electronics operating at temperatures less than one tenth of a degree above absolute zero, and all realized on a single silicon chip fabricated in a commercial semiconductor foundry.

RESEARCHERS HIT RECORD LONG-LIVED COHERENT QUANTUM STATES IN A SUPERCONDUCTING DEVICE

Researchers showed that large numbers of quantum bits, or qubits, can be tuned to interact with each other while maintaining coherence for an unprecedentedly long time, in a programmable, solid state superconducting processor. The team included members from Arizona State University and Zhejiang University in China, along with theorists from the United Kingdom.

STUDY: QUANTUM COMPUTING IN SILICON HITS 99% ACCURACY

Australian researchers have demonstrated that near error-free quantum computing is possible, paving the way to build silicon-based quantum devices compatible with current semiconductor manufacturing technology. Professor Andrea Morello of UNSW, who led the work said the team reported in Nature that the team's operations were 99 per cent error-free.

QUANTUM AI MAY NEED ONLY MINIMAL DATA — PROOF TAKES STEP TOWARD QUANTUM ADVANTAGE

Training a quantum neural network requires only a small amount of data, according to a new proof that upends previous assumptions stemming from classical computing's huge appetite for data in machine learning, or artificial intelligence. The theorem has several direct applications, including more efficient compiling for quantum computers and distinguishing phases of matter for materials discovery.

CHINESE RESEARCHERS REPORT ON HIGHLY EFFICIENT PROCESS FOR ENTANGLING PHOTONS

A team of Chinese scientists report on a new method for entangling photons that they say could make quantum networks and quantum computing more practical. In a study published in Nature Photonics, the team from the University of Science and Technology of China said that the new way to produce entangled photons is extremely efficient. The work was led by Jian-Wei Pan, one of the world's leading quantum researcher from the Hefei National Research Center for Physical Sciences at the Microscale, the University of Science and Technology of China and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China.

"Our Approach Is Advantageous Since It Is Not Only Very Resource Efficient By Merely Using A Single Setup But Also Shows Much Better Scaling Of Adding More Photons."

QUANTINUUM STUDY SHOWS LOGICAL QUBITS CAN OUTPERFORM PHYSICAL QUBITS, MAJOR

STEP TOWARD SCALABLE QUANTUM

A team of Quantinuum scientists report on an important research advance that shows logical qubits can outperform physical qubits, a key step toward quantum computers that can be used to solve practical problems. It's also an achievement that only recently was thought to be years away. The demonstration offers a path toward scalability, qubit efficiency and less circuitry needed for fault-tolerance, the team added.

NVIDIA SAYS UNIFIED COMPUTING PLATFORM WILL SPEED UP QUANTUM R&D

The NVIDIA Quantum Optimized Device Architecture, or QODA, aims to make quantum computing more accessible by creating a coherent hybrid quantum-classical programming model, according to a statement. QODA is an open, unified environment for some of today's most powerful computers and quantum processors, improving scientific productivity and enabling greater scale in quantum research.

QCI SOLVES 3,854-VARIABLE PROBLEM IN SIX MINUTES IN BMW GROUP, AWS QUANTUM COMPUTING CHALLENGE

Quantum Computing Inc. (QCI) (NASDAQ: QUBT), a leader in accessible quantum computing, today announced that it has solved an optimization problem with over 3,800 variables in six minutes, delivering a superior and feasible solution. The Company achieved this landmark by applying a new quantum hardware technology called Entropy Quantum Computing (EQC) to the BMW Vehicle Sensor Placement challenge, a complex problem consisting of 3,854 variables and over 500 constraints. In comparison, today's Noisy Intermediate Scale Quantum (NISQ) computers can process approximately 127 variables for a problem of similar complexity.

"We Believe That This Proves That Innovative Quantum Computing Technologies Can Solve Real Business Problems Today. What's Even More Significant Is The Complexity Of The Problem Solved. This Wasn't Just A Rudimentary Problem To Show That Quantum Solutions Will Be Feasible Someday; This Was A Very Real And Significant Problem Whose Solution Can Potentially Contribute To Accelerating The Realization Of The Autonomous Vehicle Industry Today." — Bob Liscouski, Ceo Of Qci

SEEQC USES FORMFACTOR'S QUBIT PRE-SCREENING SOLUTION TO SPEED QUANTUM COMPUTING DEVELOPMENT

FormFactor, Inc., a leading semiconductor test and measurement supplier, announced that SEEQC, the Digital Quantum Computing company, has deployed FormFactor's recently announced integrated measurement solution to markedly expedite its quantum computing research and development program. The measurement solution, including the sub-50mK HPD Model 106 Adiabatic Demagnetization Refrigerator (ADR) and the PQ500 RF and DC probe socket, complements sub-10mK dilution refrigerators to accelerate cryogenic test cycles by more than two times.

RESEARCHERS TELEPORT QUANTUM INFORMATION ACROSS QUANTUM NETWORK

Researchers in Delft have succeeded in teleporting quantum information across a rudimentary network. This first of its kind is an important step towards a future quantum internet. This breakthrough was made possible by a greatly improved quantum memory and enhanced quality of the quantum links between the three nodes of the network. The researchers, working at QuTech—a collaboration between Delft University of Technology and the Netherlands Organisation for Applied Scientific Research (TNO)—are publishing their findings today in the scientific journal Nature.

ERROR-MITIGATION TECHNIQUES CAN PUMP UP THE QUANTUM VOLUME

Boosting quantum volume may not be a job just for hardware makers, according to researchers from the

Unitary Fund. Quantum algorithm developers can play a role, too. In a study, the team said that they experimentally demonstrated that error mitigation improves the effective quantum volume of several different quantum computers

RESEARCHERS MAY HAVE A METHOD TO KEEP QUANTUM INFORMATION AS SAFE AS CLASSICAL INFORMATION

A team of Moscow State University-led researchers have theoretically shown that quantum information can be kept safe from errors just like classical information, according to Quanta Magazine. The team — led by Pavel Panteleev and Gleb Kalachev of Moscow State University — released its findings in ArXiv, a preprint server. The researchers combined two classical methods and invented new techniques on their own. Prior to this study, most methods to keep quantum information safe from errors could not compete with the reliable and efficient methods of classical computers.

7.Cisco Bets On Quantum Key Distribution

by Nancy Liu
https://www.sdxcentral.com/articles/interview/cisco-bets-on-quantum-key-distribution/2022/12/

Cisco Chief Strategy Officer Liz Centoni expects quantum key distribution (QKD) to gain momentum next year as organizations and governments try to address post-quantum security threats.

“Quantum cryptography and transmitting keys is a fundamental risk to security as they can be harvested and decrypted later,” Centoni wrote in her 2023 technology predictions and trends blog.

“While post-quantum cryptography (PQC) is a potential stop-gap solution, it’s unclear if PQC schemes could be broken in the future,” she added. “QKD is poised to be particularly impactful because it avoids any distribution of the keys over an insecure channel. In 2023, in preparation for a post-quantum world, we will see a macro-trend emerge with the adoption of QKD in data centers, IoT, autonomous systems, and 6G.”

Ramana Kompella, distinguished engineer and head of research in the Emerging Tech and Incubation group at Cisco, echoed this prediction and told SDxCentral that Cisco has been making strides in quantum research and development.

SDxCentral: What efforts has Cisco made on QKD development or implementation?

Kompella: Our research team is focused on a wide variety of research areas such as PQC and QKD toward securing the next-generation digital infrastructure. While PQC schemes work with classical networks, QKD requires quantum networks. Cisco Research is looking into converged networking infrastructure for both classical and quantum communication that can support QKD in the future.

We also collaborate closely with academic researchers from various top universities across the world to advance the state-of-the-art in these areas and support their research by providing funding and other resources to achieve impact.

In the past year, Cisco Research has invested in nearly a dozen Quantum projects from universities in the U.S., the U.K., and the E.U. We also recently hosted the second annual Cisco Quantum Summit – a two-day virtual event aimed at bringing together experts to discuss progress toward building the Quantum Internet.

Finally, as part of quantum research and development efforts at Cisco, we are currently accepting research proposals that aim to conduct research in different areas of quantum hardware, software, and applications.

8.Quantum Tech's Path To Commercialization Will Be A 2023 NIST Priority

by Alexandra Kelley
https://www.nextgov.com/emerging-tech/2022/12/quantum-techs-path-commercialization-will-be-2023-nist-priority/381203/

The National Institute of Standards and Technology spearheaded applied quantum research in 2022, and looks to further stand up the growing industry in the coming year.

Quantum sensing and post-quantum cryptography are two technologies that researchers at the National Institute of Standards and Technology will be prioritizing in the coming year as researchers focus on the logistics behind commercializing applied quantum technologies.

James Kushmerick, the director of NIST's Physical Measurements Laboratory, told *Nextgov* that the agency's next step for post-quantum cryptography is standardizing the quantum-resistant algorithms released earlier this year.

“Post quantum crypto, or PQC, is hugely important…and NIST has identified four algorithms which they're working through the process of standardizing…with the community,” he said. “Post quantum cryptography is definitely a high priority and there…continue[s] to be a lot of effort in that arena.”

Continuing partnerships with labs and experts in the private sector, industry, and academia will continue to help fuel new quantum sciences research, particularly within the Quantum Economic Development Consortium. In addition to the actual development of new technology, partnering institutions will also lend a holistic perspective to determine how to support quantum technologies' entrance into the commercial marketplace.

He referenced programs like NIST on a Chip, which has quantum devices and sensors to deliver precise measurements in a singular software chip. Kushmerick said that NIST is looking to form new partnerships with industry leaders to craft a durable product fit for market distribution.

Despite the demand, scalability and commercialization are two of the largest challenges scientists face.

“One of the real advantages there is we can look in the pre competitive space,” Kushmerick said. “Then we can kind of collectively solve some of these problems that are not unique to any one application or any one technology but, you know, will be needed across the board.”

Kushmerick cites the development of adjacent low-cost, low-power foundational technologies—like cryocoolers to keep quantum processing systems cool—as one example of the larger infrastructure that will need to be developed to make quantum technologies sustainable.

“A lot of quantum systems require to be cooled down, you know, close to absolute zero. So there's different ways you can do that: you can use liquid helium, you can use a dilution refrigerator. And many of these are large … laboratory-scale kind of systems. If you…need to cool down and have these in, you know, at every cell tower, let's say if you were building up a sensor network or something, you need to be able to do this at a lower size, weight and power swap kind of aspect, but also at a lower enough cost, that it's actually deployable," he said. "If it's $2 million a pop … no one's going to be able to afford that."

Despite the innovations made with quantum sensing technology and post-quantum cryptographic standards, Kushmerick noted that NIST is still researching a slew of other applications related to its core mission surrounding measurement standardization.

"We need to be there for the superconducting qubit, for the ion trapping, for the photonics, so we have programs that span all the main technology paths, so that we're cognizant and developing the metrology needed in them," he said.

Alongside maintaining industry partnerships, NIST is also focusing on promoting U.S. leadership in developing open standards to promote fair competition in emerging tech industries.

"There's entities that try to narrowly define standards to lock a market in or to keep people out of a market. So that's where really the United States as a whole needs to engage," he said.

But before any use or consensus standards come into play, Kushmerick cautioned that the mass onset of quantum technologies is still far away, citing steady federal support as the final piece of the puzzle to stand up a commercialized quantum industry.

"Quantum technology is going to take a while—even though we have individual qubits and things like that—to really scale up and that we need to, you know, have consistent effort from across the government to really make that happen," he said. "We have to take this long approach to it."

9.Encryption Is A Societal Question…Needs Healthy Debate Among Govt, Cos And Citizens: Royal Hansen

by Soumyarendra Barik
https://indianexpress.com/article/technology/tech-news-technology/encryption-is-a-societal-question-needs-healthy-debate-among-govt-cos-and-citizens-royal-hansen-8333518/

A number of threats that India faces in cyberspace are similar to what the United States or Europe typically face, and India should get rid of legacy digital infrastructure to become more resilient to cyberattacks, Royal Hansen, Google's vice president of engineering for privacy, safety, and security said. In an interview with the author, Hansen also spoke about the threat from foreign state actors, some of the unique challenges that India's cyberspace faces, and Google's stand on the encryption debate. Edited excerpts:

There is said to be the involvement of a foreign state actor in the recent cyberattack on AIIMS. Are foreign states today the biggest actors in cyberspace, or are they mostly independent actors?

Google's Threat Analysis Group (TAG) and Mandiant, which we acquired earlier this year, track around 300 nation state groups. And we see threats from nation state actors continue to grow. The big players remain to be big, but what's also happened is that smaller states are also buying exploits and acting bigger. So it is becoming a bigger and bigger issue not because armies are growing in each of these countries. It's the ecosystem of people buying and selling exploits, data, compromising botnets etc. The lines are becoming very blurry. InIndia's case, it is just like in the USA, that when you are a big player, writing software for the world, and your economy is growing, you are going to be on the attackers' list. So, Google will be training 40,000 developers on writing secure software. India should also get rid of legacy infrastructure so that the country is more resilient to cyberattacks.

Is Google having conversations with the Indian government on cybersecurity and how to make their systems more secure?

One of the reasons Google's global senior leadership is in India is to have meetings with the government along those lines. We will share threat intelligence on things like high end attackers and the trends we are seeing and how we are baking that threat intelligence into our products like Google Pay and Gmail.

What do you think is the biggest cyber threat facing India today? Is it unique to the country?

One of the main issues is the use of legacy infrastructure which is a common trend across the world, not just India. These systems typically become the first point of attack. The difference in India is not the type of attacks, but the pace at which the country has grown. There are more new people participating, businesses growing. So it becomes that much more important that we don't use legacy systems. You have to be secure by default. Along with that the products also have to be safe.

Companies like Apple and Meta's WhatsApp have taken essentially a very pr-encryption stance in their products and services. Does Google also think that end-to-end encryption should be the norm for most digital services? Or should there also be consideration for law enforcement purposes and baking some kind of accessibility?

The most important thing is not to view this as just a technical problem. We are talking about societal questions. There is a tendency to say that one technology or one implementation can solve it. Like we have seen in other industries like aviation, naval, healthcare etc. there are always tricky tradeoffs. To me, it is important that governments, companies, tech platforms, and citizens have a healthy debate. I am in favour of a societal approach.

Encryption is a tool and we use it in certain cases. But do I think everything in the world will be end-to-end encrypted? No, because then services can't be rendered. Yes, there is absolutely a time and place for end-to-end encryption, but what lots of people also want is for a service provider to see and act on their data so that they can give them a convenience.

It is a healthy debate that society needs to have, and we're not the arbiters of that. I want it to be a societal question.

10.Top 11 Predictions For 2023'S Quantum Technology Industry

by Matt Swayne
https://thequantuminsider.com/2022/12/20/top-11-predictions-for-2023s-quantum-technology-industry/?utm_source=newsletter&utm_medium=email&utm_term=2022-12-28&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Quantum+2022+in+Review+Quantum+Predictions+for+2023+And+M

ore+Quantum+News

If quantum mechanics teaches us anything, it's that uncertainty rules reality.

So, it's always a risk making prediction about anything, but trying to make accurate predictions in an industry that relies on the fuzzy probabilities of quantum mechanics is exceedingly difficult.

But, after spending 3-plus years covering quantum and after what seems like a lifetime reading about the wonders of quantum science and quantum computing, I feel the irresistible urge to pull back the veil on 2023 and try to guess what's coming up.

If you are looking for a methodology, there really isn't one. It's not exactly a dart board. But, this is a matter of gathering information about micro research advances and financial trends, then add some more obvious macro economic trends — and then putting those on the dart board.

Here's what I came up with.

The Runway Runs Out

Billions of dollars in investment money have primed the quantum startup pump. Not all of these startups were ready for that injection of funds. Technologically, some of these firms may be some years away from a real product. Investment vehicles, such as special purpose acquisition companies, were weakened by a choppy economy and failed to fully fund quantum startups. Investors in these SPACs called in reimbursements, a financial equivalent of pulling the rug out of entrepreneurs. On the macro side, federal banks are pulling in their COVID-era bias toward low-interest rates in hopes of cooling inflation. All of this will mean that several quantum startups could either run out of money, or may need to drastically curb spending and limit their ambitions. This threat may ease somewhat with a return of liquidity to the market and the recognition that quantum tech is integral to national security. Still, the risks are high for startups to sputter in 2023 and, in some cases, sputtering out of existence.

Creative Construction

The waves of disruption that have spread through the economy — supply chain woes, crypto crashes and general investing malaise — will catch up to the relatively unscathed quantum in 2023. It's easy to look at that as a singularly negative input, but it's not. Challenging economics can force creative workarounds, solidify innovative partnerships and generally make people work harder to attain market advantage. There will be lots of news about companies making interesting — and sometimes contrarian — moves to first, stay afloat and, second, keep sailing.

Merge, Baby Merge

One of the ways that companies will deal with the economic forces and competitive pressures will be to form new alliances. Some of these will be commercial agreements — temporary partnerships and collaborations, for example. But, expect to see headlines about companies merging and other companies being acquired. Software companies will join with hardware companies. Companies that target a specific approach or use case — let's say post-quantum cryptography — may link with companies working on other uses to offer the customer a wider spectrum of solutions.

Hybrid Merge

Quantum computers work well for certain problems, but classical computing is more practical for other computational problems. This year, more high-performance computing centers will add quantum to their offerings. This will begin to create new HPC-Plus or, maybe, HPC-Q centers. We see more HPC providers at least testing quantum waters in 2023 — and perhaps a few others will be bouncing off the high-dive, pulling into a cannonball and entering the quantum pool with a huge splash in the coming year.

Taking Down The Chandelier

Something a little different here.

The golden chandelier has been an evocative image for quantum computing, even though it is most associated with a single modality, superconducting quantum. It's a bit misleading, though. Companies that offer other modalities — neutral atom and photonic, for sake of example — will grapple with branding their own devices as quantum computers without the chandelier.

This isn't a frivolous as it might sound. Branding is a powerful tool and a powerful obstacle. Quantum science and quantum business must penetrate the mass public's perception of the technology. Funders and investors are likely in that mass public and share those perceptions.

In 2023, expect some of the companies that back alternative modalities to explore ways to make their cool technology — although perhaps not as sexy as a golden chandelier — more evocative with the public.

Don't look for this trend as a way to pick a winner among the competing quantum modalities. We're a long way off for selecting a quantum approach — or approaches — that will dominate the space.

C.E.-Go

Deep tech companies have a unique origin story. Almost all of them started in the mind of a scientist and emerged out of a lab. Not a business school. Not a garage. Not a tech accelerator. As quantum startups grow, some founders may realize they do not have the business acumen to lead international, billion-dollar businesses. These founders may step aside to bring on executives with more business experience. Others will persevere and — hopefully — transition successfully. Others will be replaced. This CEO form of musical chairs will likely have a unforeseen benefit. Quantum companies may pull CEO candidates from other technological fields and different industries, meaning that current networks will expand to include more domain experts, who will then explore the use of quantum in their previous industries.

National Security Buoys Quantum

The story of military history is, at heart, the story of technological innovation. Whether it's the composite bow of the Mongols, the horse-riding acumen of the Comanches, the cryptographic skill of the British in World War II, or the stealth technology of today, the ability to create and master advanced technologies offers an immediate battlefield advantage. As mentioned, we expect a lack of liquidity to hamper commercial investment in quantum, at least in the near future. However, governments will not abandon funding quantum technologies. There is a real sense that quantum technologies — such as quantum computing, quantum sensors, quantum communication and quantum cryptography — are one breakthrough away from practical use. The nation, or nations, that adopt it will have a definite advantage in national security. The countries that walk away from quantum at this vital moment in its development… will not.

Research Surprise

This is the wild card. And we have no idea when or who will play this card. But researchers are circling two critical roadblocks to quantum advantage — qubit number and error correction are two significant challenges. Any sudden significant advance in these two — so long as they can be implemented in a scalable way — means that quantum technology will mature quickly and the quantum market will expand rapidly. If that happens in 2023, most of the other predictions will be subject to revision.

More Post-Quantum Interest

2022 was the year that mainstream businesses discovered post-quantum cryptography, or PQC. They discovered PQC simply because there's a business case for the investment. The hack-now-decrypt later is a rallying cry for teams who want their PQC projects funded. Expect that to continue and grow in 2023 and it may lead to broader quantum adoption. See our next prediction

PQC Ed Spread

The most practical business case for quantum computers — at least right now — is preparing to stop quantum computers, at least ones trying to hack into your vital organizational data. But, also expect some leakage here. In other words, teams that companies are bringing together to learn about how to defeat would-be quantum hackers are also learning about the potential for quantum computers to accomplish good — massively improving drug discovery, mastering financial risk, helping scientists explore materials, etc. Those teams will likely spread this information to other workers in their organizations. Smart companies are going to nurture this cross-company, interdisciplinary collaborations and find places for quantum innovation within the company. This may even spawn entirely new categories of use cases for quantum as deep quantum understanding meets real world domain expertise.

Navigating Complexity Becomes an Issue

Currently, the quantum ecosystem is kind of a beautiful mess. There are multiple modalities, dozens of software languages, a range of equipment needs to build and control qubits, etc. That's the result of pure innovation: Start-ups and research institutions are jumping into the fray and building things on the fly. For end users, though, "beautiful" is probably not the right adjective. It's just a mess. And some sorting out will be needed. Consolidation and mergers — as discussed above — may help the simplest, domain user-friendly approaches rise to the top. And the others, well, Mr. Schumpeter will take it from here.

11.Quantum Researchers Discover The And Gate

by Charles Q. Choi
https://spectrum.ieee.org/quantum-and-gate

As powerful as quantum computers may one day prove, quantum physics can make it challenging for the machines to carry out quantum versions of the most basic computing operations. Now scientists in China have created a more practical quantum version of the simple AND operation, which may help quantum computing reach successful near-term applications.

Conventional electronics nowadays rely on transistors, which flick on or off to symbolize data as ones and zeroes. They connect transistors together to build devices known as logic gates, which implement logical operations such as AND, OR, and NOT. Logic gates are the building blocks of all digital circuits.

In contrast, quantum computers depend on components known as quantum bits or "qubits." These can exist in a quantum state known as superposition, in which they are essentially both 1 and 0 at the same time. Quantum computers work by running quantum algorithms, which describe sequences of elementary operations called quantum logic gates applied to a set of qubits.

Superposition essentially lets each qubit perform two calculations at once. The more qubits a quantum computer has, the greater its computational power can grow in an exponential fashion. With enough qubits, a quantum computer could theoretically vastly outperform all classical computers on a number of tasks. For instance, on quantum computers, Shor's algorithm can crack modern cryptography, and Grover's algorithm is useful for searching databases at sometimes staggering speeds.

However, quantum computers face a physical limitation: All quantum operations must be reversible in order to work. In other words, a quantum computer may perform an operation only if it can also carry out an opposite operation that returns it to its original state. (Reversibility is necessary until a quantum computation is run and its results measured.)

In everyday life, many actions are reversible—for example, you can both tie and untie shoelaces. Others are irreversible—for instance, you can cook an egg but not uncook it.

Similarly, a number of logical operations are reversible—you could apply the NOT operation to a variable and then apply it again to return it to its original state. Others are generally irreversible—you could add 2 and 2 together to get an outcome of 4, a mathematical version of the AND operation, but you could not reverse the operation and know an outcome of 4 began as 2 and 2 unless you knew what at least one of the original variables was.

The AND gate is a fundamental ingredient of both classical and quantum algorithms. However, the demand for reversibility in quantum computing makes it challenging to implement. One workaround is to essentially use an extra or "ancilla" qubit for each AND gate that stores the data needed to reverse the operation.

However, quantum computers are currently noisy intermediate-scale quantum (NISQ) platforms, meaning their qubits number up to a few hundred at most and are error-ridden as well. Given quantum computing's primitive state right now, it would prove "extremely cumbersome to design and build hardware for accommodating extra ancilla qubits on an already crowded processor," says study cosenior author Fei Yan, a quantum physicist at the Southern University of Science and Technology in Shenzhen, China.

Now Yan and his colleagues have constructed a new quantum version of the AND gate that removes this need for ancilla qubits. By getting rid of this overhead, they say, their new strategy could make quantum computing more efficient and scalable than ever.

"Our work will help narrow the gap between the most anticipated near-term applications and existing noisy devices," Yan says. "We hope to see quantum AND functionality added to quantum programs on machines elsewhere, such as the IBM quantum cloud, and played with by more people."

Instead of using ancilla qubits, the new quantum AND gate relies on the fact that qubits often can encode more than just zeroes and ones. In the new study, the researchers have qubits encode three states. This extra state temporarily holds the data needed to perform the AND operation. "We do not use any ancilla qubits," Yan says. "Instead, we use ancilla states."

In the new study, the scientists implemented quantum AND gates on a superconducting quantum processor with tunable-coupling architecture. Google also employs this architecture with its quantum computers, and IBM plans to start using it in 2023.

"We think that our scheme is well-suited for superconducting qubit systems where ancilla states are abundant and easy to access," Yan says.

In experiments, the researchers used their quantum AND gate to help construct Toffoli gates, with which quantum computers can implement any classical circuit. Toffoli gates are key elements of many quantum-computing applications, such as Shor's and Grover's algorithms and quantum error-correction schemes.

In addition, with six qubits the researchers could run Grover's algorithm on a database with up to 64 entries. "To our knowledge, previous demonstrations of Grover's search on any system was limited to 16 entries," Yan says. This highlights the way in which the quantum AND operation can help scale up quantum computing, he adds.

All in all, "what we really want to emphasize is that our technique presents a scaling advantage," Yan says. "The more qubits are involved, the more cost-saving our technique would be compared to the traditional one."

Although these experiments were conducted with superconducting qubits, Yan notes that their quantum AND gate could get implemented with other quantum-computing platforms, "such as trapped ions and semiconductor qubits, by utilizing appropriate ancilla levels."

The scientists detailed their findings online 14 November in the journal *Nature Physics*.

12.Google Introduces End-To-End Encryption For Gmail On The Web

by Sergiu Gatlan
https://www.bleepingcomputer.com/news/security/google-introduces-end-to-end-encryption-for-gmail-on-the-web/

Google announced on Friday that it's adding end-to-end encryption (E2EE) to Gmail on the web, allowing enrolled Google Workspace users to send and receive encrypted emails within and outside their domain.

Client-side encryption (as Google calls E2EE) was already available for users of Google Drive, Google Docs, Sheets, Slides, Google Meet, and Google Calendar (beta).

Once enabled, Gmail client-side encryption will ensure that any sensitive data delivered as part of the email's body and attachments (including inline images) can not be decrypted by Google servers — the email header (including subject, timestamps, and recipients lists) will not be encrypted.

"You can use your own encryption keys to encrypt your organization's data, in addition to using the default encryption that Google Workspace provides," Google explained on its support website.

"With Google Workspace Client-side encryption (CSE), content encryption is handled in the client's browser before any data is transmitted or stored in Drive's cloud-based storage.

"That way, Google servers can't access your encryption keys and decrypt your data. After you set up CSE, you can choose which users can create client-side encrypted content and share it internally or externally."

Gmail E2EE beta is currently available for Google Workspace Enterprise Plus, Education Plus, and Education Standard customers.

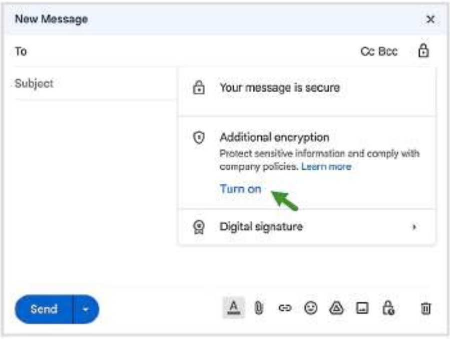
They can apply for the beta until January 20, 2023, by submitting their Gmail CSE Beta Test Application which should include the email address, Project ID, and test group domain.

The company says the feature is not yet available to users with personal Google Accounts or Google Workspace Essentials, Business Starter, Business Standard, Business Plus, Enterprise Essentials, Education Fundamentals, Frontline, and Nonprofits, as well as legacy G Suite Basic and Business customers.

After Google emails back to confirm that the account is ready, admins can set up Gmail CSE for their users by going through the following procedure to set up their environment, prepare S/MIME certificates for each user in the test group, and configure the key service and identity provider.

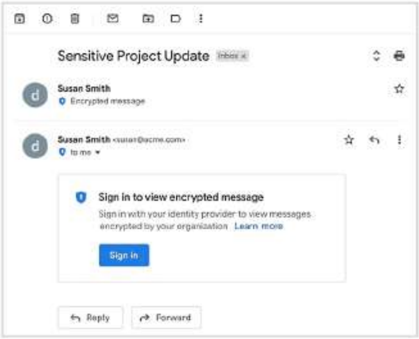
The feature will be off by default and can be enabled at the domain, organizational unit, and Group levels by going to Admin console > Security > Access and data control > Client-side encryption.

Once enabled, you can toggle on E2EE for any message by clicking the lock icon next to the Recipients field and clicking "Turn on" under the "Additional encryption" option.



Your message is secure

Additional encryption
Protect sensitive information and comply with company policies. Learn more



Susan Smith
Encrypted message

Susan Smith <susan@acme.com>
to me

Sign in to view encrypted message
Sign in with your identity provider to view messages encrypted by your organization. Learn more

Users will then be able to compose their Gmail messages and add email attachments as they would normally do.

"Google Workspace already uses the latest cryptographic standards to encrypt all data at rest and in transit between our facilities," Google added.

"Client-side encryption helps strengthen the confidentiality of your data while helping to address a broad range of data sovereignty and compliance needs."

13.Semiconductor Industry 'Wakes Up' To Quantum Threats

by Nancy Liu
https://www.sdxcentral.com/articles/interview/semiconductor-industry-wakes-up-to-quantum-threats/2022/12/

Lattice Semiconductor three years ago launched its security business. Now, it plans to introduce quantum-resistant field-programmable gate array (FPGA) devices to its server customers.

Mamta Gupta, director of portfolio management at Lattice Semiconductor, told SDxCentral that she expects the breakthrough in quantum computer development will come much sooner than others think, and the semiconductor industry is waking up to that fact.

SDxCentral: What did Lattice Semiconductor do for quantum security?

Gupta: For quantum computing, initially it was thought that it's going to be somewhere in 2030 or beyond, and then suddenly be woken up to the fact that 2030 is not that far away and the quantum computers are outpacing or the development of them is outpacing all the estimates. So now this decade, the decade of 2020s, has been called the quantum decade. And people are realizing that the threat that is emerging from post-quantum computing is very real and is very near. So if you're going to do any system or release any system that will be in operation in 2025, it has to be post-quantum capable or quantum-resistant because it will stay in the market for five to 10 years and by that time viable quantum computers will be in the market.

So with that in mind, we recognize that threat pretty early on. And today we have implemented multiple quantum-resistant algorithms in our FPGAs for asymmetric cryptography. So we have implemented NIST-approved quantum-resistant algorithms in asymmetric cryptography or public key cryptography, which is the most vulnerable for quantum computers. It's like a bullet to a paper. The quantum computers will just pierce through asymmetric crypto.

We have symmetric crypto hardened in our devices and we are participating in the ecosystem for post-quantum cryptography to establish our incumbency by 2023.

SDxCentral: How is quantum computing impacting FPGA and the broader semiconductor industry?

Gupta: There is a lot of activity that is going on, and if you see all the major players who make processors or implement data centers they all have announced their quantum initiatives. You can take all the big names and they have a quantum strategy or some quantum roadmap and some are actually building like IBM, Intel, Fujitsu, and Google. They have put their bets on a quantum computer and they openly publish their roadmaps and all these are industry leaders and they are charging ahead with the technology.

But then you need a lot of ecosystem around it. And we see that a lot of software companies and artificial intelligence (AI) companies are stepping in to do the orchestration that will be needed for these quantum computers. So we do see the drumbeat getting louder and louder. And when this called for industry players to partner with it, we saw all the big names who are collaborating with NIST or the National Cyber Security Center of Excellence to do the migration to post-quantum cryptography projects. We see Amazon, we see Cisco, we see Microsoft, Samsung, VMware … these are all the industry leaders, they're all engaging with the National Cybersecurity Center of Excellence.

SDxCentral: When do you think quantum resistance will become a differentiator among semiconductor vendors?

Gupta: Today, the industry is waking up to it but the governments have already woken up to it. They are very well aware of the threat that is underway because they are state actors, they have to protect the critical infrastructure, so that it's not about commercial differentiation. At this time it is almost about being compliant with government mandates, and we are seeing a lot of government mandates. There was this White House memo that came out and it's asking for all of its agencies to be quantum-compliant or post-quantum compliant to the new architecture for all their new software by 2025, and the timeline is so close.

And if you want to do business with the U.S. government, for any system to be released in 2025, it has to be designed now. So it's already becoming a mandate to engage. To anybody who will engage with infrastructure projects or engage with the U.S. government, their projects already need post-quantum solutions.

So any company that is making data centers for public use is already looking for post-quantum solutions for systems, so that's where AWS and Microsoft are engaging to do this migration to post-quantum reality. So we will work with all of these vendors. They are already looking for solutions and this is where if we can provide them that we already have a differentiation.

14.Ture Shares 9 Cybersecurity Predictions For 2023

by Tim Keary
https://venturebeat.com/security/accenture-cybersecurity/

With a recession potentially looming in 2023, enterprises are feeling the squeeze to bolster their cyber resilience to avoid unpleasant surprises, with cybersecurity experts anticipating an uptick in cybercrime.

Recently, VentureBeat caught up with some of Accenture's top cybersecurity experts, who outlined their security predictions for 2023.

Accenture's predictions include growth in: destructive and non-financially motivated cyberattacks; the cybersecurity talent pool; automated response technology; and "steal now, decrypt later" quantum threats.

Below is an edited transcript of their responses.

1. **Geopolitics, economic uncertainty and destructive cyberattacks will challenge leads to step up**

   "Economic uncertainty and heightened global tensions will fuel a resurgence of cyberattacks from groups that are becoming increasingly structured, organized and destructive," said Paolo Dal Cin, global lead at Accenture Security. "While the ransomware trend will continue, we believe it will be less focused on profit and more on wreaking havoc and destroying data."

   Also unfortunately, the barrier to entry for would-be threat actors is now even lower, because the malware is being written through natural language processing (NLP) supported by artificial intelligence (AI), he said.

   The seeds of some of these trends were planted with Russia's invasion of Ukraine, when Accenture's cyber threat Intelligence team uncovered a significant increase in hacktivist activity targeting Western entities.

   "The good news: We believe this geopolitical unrest and the nature of destructive cyberattacks should, and likely will, accelerate allied countries' efforts to share more threat intelligence information," said Dal Cin.

Furthermore, the ability and willingness to share information on zero-day vulnerabilities and third-party cyber incidents will become foundational to security as attackers focus on national infrastructure, he said.

2. Evolving threat tactics require renewed focus on digital identity

"With more organizations armed with strong endpoint protection software, cyberattack techniques will likely evolve to evade sophisticated detection technologies," said Robert Boyce, global cyber resilience lead at Accenture. "As detection technology becomes a standard, threat actors are thinking outside the box."

In 2023, he expects to see more tactics that involve legitimate access to a corporate network that no longer involve deploying malware. The focus will be on living-off-the-land techniques to exploit what is already available in the victim environment.

"Threat actors will either buy access or use social engineering techniques to gain access to a network and avoid detection [by] leveraging a standard user profile for the company to pass off as an employee," said Boyce.

Significant damage can be done without sophisticated malware, he said. So organizations need to be thinking ahead about their identity fundamentals, and how they can implement more detection and protection controls.

"It will be more critical than ever to have a baseline understanding of typical user behaviors associated with users or groups of users to identify the anomalies," said Boyce.

3. Broader talent pools will strengthen cybersecurity

"Given our work, we know well the challenges of hiring skilled professionals to meet market demand, and have learned to adapt what we do to attract and retain the best cybersecurity talent," said Ryan LaSalle, North America security lead at Accenture. "To widen the talent pipeline in 2023, employers will expand beyond degrees to evaluate candidates based on their skills, experience and potential."

He expects that employers will modify job descriptions to reflect what is truly required to enter the cyber workforce. He predicts leading organizations will invest more in programs connecting to higher education and other industry partners that can work together to identify untapped sources of talent and develop cyber professionals where they may not already exist.

Apprenticeship programs, upskilling programs and public-private partnerships will also play a major role in unlocking cyber talent in the new year, he said. "This will improve diversity in cybersecurity, which in turn will drive increased innovation and better protect our communities."

4. Protecting people: Cybersecurity for critical infrastructure will take a central role

"In 2023, critical infrastructure will remain a prime target for cyber adversaries and individual bad actors," said Jim Guinn, global cyber industry (including OT/IoT) lead at Accenture. "Plain and simple, this means more lives will be at stake."

Critical infrastructure organizations will need to sharpen their focus on regulatory compliance, he said, including creating an enduring program to understand and comply with a growing list of regulations across a growing number of jurisdictions.

"This will require organizations to lean in and work collaboratively with governments and regulators, including advising working groups and policymakers on industry-specific needs to ensure that regulations are as effective as possible without over-burdening organizations," said Guinn.

5. **Increasingly automated responses will become core tech for the cyber-resilient business**

   "As the cyber threat landscape evolves, we will see the number of cyber events and organizations held to ransom continue to rise," said James Nunn-Price, growth markets security lead at Accenture. "With this increase, organizations will continue to make significant investments in their situational awareness, threat-based security monitoring, incident response and crisis management practices."

   However, many organizations, including those with mature practices, are still overly reliant on people, and that can slow detection and responses, he said. For example, Accenture found that even when security monitoring teams took action to mitigate attacks, it was still too late to stop data exfiltration.

   Attackers are using the latest tools and automated technologies to strike fast and hard — to exfiltrate key data and damage infrastructure within minutes.

   "In 2023, more organizations will prioritize fully automated response technology, as the impacts from a successful breach now far outweigh the risks of these newer technologies, which in turn, frees their people up to focus on how the business can become more cyber resilient, said Nunn-Price.

6. **Bring on the boards: Those at the very top will dive more deeply into cyber oversight and reporting**

   "As we head into 2023, we expect the expanding cyber risk environment and increasingly complex regulatory environment to energize boards," said Valerie Abend, global cyber strategy lead at Accenture. "They'll become much more persistent and intentional, moving from quarterly or annual updates to routinely contemplating cyber risk across all areas of the business and management's efforts."

   In turn, she said, this will prompt other members across the C-suite to "up-level their knowledge and active involvement in managing this risk environment."

7. **Locking down cloud security: Look for more innovation and cooperation**

   "Cloud service providers are providing more security service features that meet compliance standards, and at the same time, third-party cloud security providers are going the extra mile by focusing on product innovation and integration with cloud platforms," said Dan Mellen, global cloud and infrastructure security lead at Accenture.

   A practical example, he said, is the cloud service provider driving easy, natural consumption of cloud security services and expanding many native security services into a commodity state causing acceleration of third-party security product feature backlog through development roadmaps to remain competitive.

   "These complimentary trends will result in improved security and control coverage — with the added bonus of increased flexibility," said Mellen.

8. **Quantum realities: New computing capabilities will require new levels of security**

   "Progress in quantum computing is bringing adversaries ever closer to a 'cryptographically relevant quantum computer' able to crack all — yes, all — of the public key encryption that protects most everything in government, industry and the internet," said Tom Patterson, global quantum and space cybersecurity lead at Accenture.

The growing danger in 2023 will be more "steal now, decrypt later" thefts of fully encrypted sensitive information, he said. The idea is that even if the stolen information can't be deciphered now, advances in quantum computing will soon crack the keys.

"Fortunately, 2023 will also see the early development and adoption of new post-quantum encryption algorithms, thus enhancing resilience, integrity and privacy even in the quantum computing age ahead," said Patterson.

9. Cybersecurity training will be applied to specific roles and business environments

"Fundamentally, the industry is struggling to connect the realities of adult learning best practices for cybersecurity with how organizations need to run their businesses efficiently and effectively," said Shelby Flora, cyber resilience talent and organization lead and UK cyber protection at Accenture.

The industry needs to shift toward identifying the pockets of the organization that need a bit more attention — including focused education and re-skilling — and then reduce friction and give time back to the business in the pockets that are showing a lower human risk, said Flora.

"In 2023, more organizations will start to shift cybersecurity training content and approaches to a more customized training experience geared toward the trainee's role and their business responsibilities," said Flora. "This means moving beyond 'how to spot a phishing email' training to more sophisticated education to better build employee awareness."

15.A Roadmap For Quantum Interconnects

by Matt Swayne
https://thequantuminsider.com/2022/12/15/q-next-releases-roadmap-for-the-development-of-quantum-information-technologies/?utm_source=newsletter&utm_medium=email&utm_term=2022-12-18&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+SpinQ+Right+Round+Senate+Passes+Cybersecurity+Bill+And+More+Quantum+News

Quantum technologies are expected to become part of our everyday lives in the coming decades. Researchers in the emerging area of quantum information science (QIS) are rapidly developing many of these technologies, including ultraprecise quantum sensors that could propel fundamental science and medicine forward by leaps and bounds; powerful quantum computers to tackle insoluble problems in finance and logistics; and quantum communications to connect these machines as part of long-distance networks.

To guide the development of these devices, the Q-NEXT quantum research center has published a new report, "A Roadmap for Quantum Interconnects," which outlines the research and scientific discoveries needed to develop the technologies for distributing quantum information on a 10- to 15-year timescale.

Q-NEXT is a U.S. Department of Energy (DOE) National Quantum Information Science Research Center led by DOE's Argonne National Laboratory.

In QIS, researchers manipulate the quantum features of nature for practical applications such as computing. The roadmap is intended to guide the QIS community as it navigates the challenges and opportunities afforded by advances in QIS.

The roadmap specifically focuses on quantum interconnects, devices that link and distribute quantum information between systems and across distances to enable quantum computing, communications and sensing.

“The role of Q-NEXT and the other DOE National QIS Research Centers is to do the science that will be useful for the public good,” said Supratik Guha, who led the roadmap effort and who is also the Q-NEXT chief technology officer, a senior advisor to Argonne’s Physical Sciences and Engineering directorate, and a professor at the University of Chicago’s Pritzker School of Molecular Engineering. “That’s why we need a roadmap. It captures the major challenges going forward and what should be done to address them.”

The roadmap comprises three sections, focused on quantum interconnect use in quantum computing, communication and sensing. Each section identifies the science and technology imperatives needed to advance the research area over the next decade; lays out the components and systems they use; poses questions that need to be addressed by the community; and outlines the developments necessary to turn the technology to practical advantage.

“Quantum information research has been mostly about the science until recently. Now, especially over the past decade, there’s been increased interest in turning the science into technology,” Guha said. “We’ve tried to be nonprescriptive, but we do say what needs to happen to build the technologies. We’ve tried to identify areas of science that need to be advanced and describe engineering challenges that need to be tackled.”

Thirty-nine experts from 15 institutions across the national labs, academia and industry contributed to the report.

“The roadmap was an excellent way to get together scientists and engineers, industry-focused and academic-focused people, to provide all points of view and learn from each other’s perspectives,” Guha said.

“We expect this roadmap will be a guide for the global QIS community as we design and develop viable quantum technologies,” said Jennifer Dionne, who is a report co-author, one of the leaders of the Q-NEXT collaboration and a professor at Stanford University. “The roadmap brings together the insights of experts spanning a broad range of disciplines. We hope it provides an integrated view to inform the strategies of national science agencies, academia and industry as they invest in this burgeoning field.”

This work was supported by the U.S. Department of Energy Office of Science National Quantum Information Science Research Centers as part of the Q-NEXT center.

16.NIST Retires SHA-1 Cryptographic Algorithm

by Chad Boutin

https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm

The SHA-1 algorithm, one of the first widely used methods of protecting electronic information, has reached the end of its useful life, according to security experts at the National Institute of Standards and Technology (NIST). The agency is now recommending that IT professionals replace SHA-1, in the limited situations where it is still used, with newer algorithms that are more secure.

SHA-1, whose initials stand for "secure hash algorithm," has been in use since 1995 as part of the Federal Information Processing Standard (FIPS) 180-1. It is a slightly modified version of SHA, the first hash function the federal government standardized for widespread use in 1993. As today's increasingly powerful computers are able to attack the algorithm, NIST is announcing that SHA-1 should be phased out by Dec. 31, 2030, in favor of the more secure SHA-2 and SHA-3 groups of algorithms.

"We recommend that anyone relying on SHA-1 for security migrate to SHA-2 or SHA-3 as soon as possible," said NIST computer scientist Chris Celi.

SHA-1 has served as a building block for many security applications, such as validating websites — so that when you load a webpage, you can trust that its purported source is genuine. It secures information by performing a complex math operation on the characters of a message, producing a short string of characters called a hash. It is impossible to reconstruct the original message from the hash alone, but knowing the hash provides an easy way for a recipient to check whether the original message has been compromised, as even a slight change to the message alters the resulting hash dramatically.

Today's more powerful computers can create fraudulent messages that result in the same hash as the original, potentially compromising the authentic message. These "collision" attacks have been used to undermine SHA-1 in recent years. NIST has announced previously that federal agencies should stop using SHA-1 in situations where collision attacks are a critical threat, such as for the creation of digital signatures.

As attacks on SHA-1 in other applications have become increasingly severe, NIST will stop using SHA-1 in its last remaining specified protocols by Dec. 31, 2030. By that date, NIST plans to:

- Publish FIPS 180-5 (a revision of FIPS 180) to remove the SHA-1 specification.
- Revise SP 800-131A and other affected NIST publications to reflect the planned withdrawal of SHA-1.
- Create and publish a transition strategy for validating cryptographic modules and algorithms.

The last item refers to NIST's Cryptographic Module Validation Program (CMVP), which assesses whether modules — the building blocks that form a functional encryption system — work effectively. All cryptographic modules used in federal encryption must be validated every five years, so SHA-1's status change will affect companies that develop modules.

"Modules that still use SHA-1 after 2030 will not be permitted for purchase by the federal government," Celi said. "Companies have eight years to submit updated modules that no longer use SHA-1. Because there is often a backlog of submissions before a deadline, we recommend that developers submit their updated modules well in advance, so that CMVP has time to respond."

17.U.S. Congress Passes The Quantum Computing Cybersecurity Preparedness

Act

https://quantumcomputingreport.com/u-s-congress-passes-the-quantum-computing-cybersecurity-preparedness-act/

The U.S. Congress has been working on a bill to have the Office of Management and Budget (OMB) to help prioritize the migration of government agency information technology systems to post-quantum cryptography. The bill contains the following provisions:

- Require the Office of Management and Budget (OMB) to prioritize the acquisition and migration of federal agencies' information technology to post-quantum cryptography;
- Instruct OMB to create guidance for federal agencies to assess critical systems one year after the National Institute of Standards and Technology (NIST) issues planned post-quantum cryptography standards;
- Direct OMB to send an annual report to Congress that includes a strategy on how to address post-quantum cryptography risks, the funding that might be necessary, and an analysis on whole-of-government coordination and migration to post-quantum cryptography standards and information technology.

Both the U.S. House and Senate have passed the bill and are expected to send it shortly to President Biden for signature. You can read the full bill and status on the Congress' website here.

18.Classical Vs. Quantum Computing: What Are The Differences?

by Ryan Arel
https://www.techtarget.com/searchdatacenter/tip/Classical-vs-quantum-computing-What-are-the-differences

As new technologies develop and gain traction, the public tends to divide into two groups: those who believe it will make an impact and grow, and those who don't. The former tends to be correct, so it is crucial to understand how future technologies differ from the status quo to prepare for their adoption en masse.

Classical computing has been the norm for decades, but in recent years, quantum computing has continued to rapidly develop. The technology is still in its early stages, but has existing and many more potential uses in AI/ML, cybersecurity, modeling and other applications.

It might be years before widespread implementation of quantum computing. However, explore the differences between classical vs. quantum computing to gain an understanding should the technology become more widespread.

Differences between classical computing vs. quantum computing

Quantum computers typically must operate under more regulated physical conditions than classical computers because of quantum mechanics. Classical computers have less compute power than quantum computers and cannot scale as easily. They also use different units of data -- classical computers use bits and quantum computers use qubits.

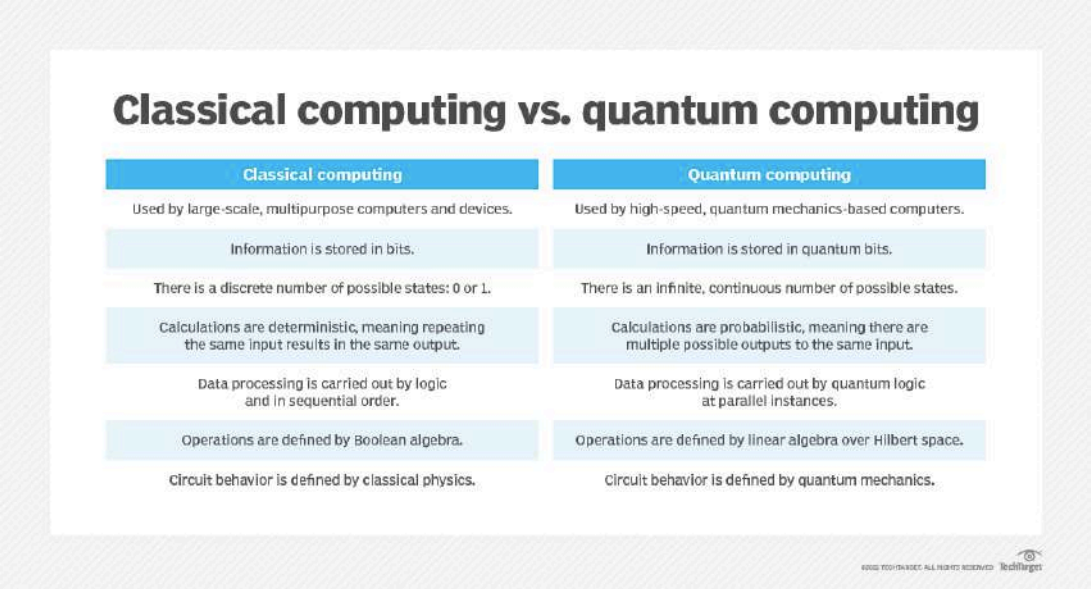
Units of data: Bits and bytes vs. qubits

In classical computers, data is processed in a binary manner.

Classical computers use bits -- eight units of bits is referred to as one byte -- as their basic unit of data. Classical computers write code in a binary manner as a 1 or a 0. Simply put, these 1s and 0s indicate the state of on or off, respectively. They can also indicate true or false or yes or no, for example.

This is also known as serial processing, which is successive in nature, meaning one operation must complete before another one follows. Lots of computing systems use parallel processing, an expansion of classical processing, which can perform simultaneous computing tasks. Classical computers also return one result because bits of 1s and 0s are repeatable due to their binary nature.

Quantum computing, however, follows a different set of rules. Quantum computers use qubits as their unit of data. Qubits, unlike bits, can be a value of 1 or 0, but can also be 1 and 0 at the same time, existing in multiple states at once. This is known as superposition, where properties are not defined until they are measured.



Classical computing vs. quantum computing

Classical computing	Quantum computing
Used by large-scale, multipurpose computers and devices.	Used by high-speed, quantum mechanics-based computers.
Information is stored in bits.	Information is stored in quantum bits.
There is a discrete number of possible states: 0 or 1.	There is an infinite, continuous number of possible states.
Calculations are deterministic, meaning repeating the same input results in the same output.	Calculations are probabilistic, meaning there are multiple possible outputs to the same input.
Data processing is carried out by logic and in sequential order.	Data processing is carried out by quantum logic at parallel instances.
Operations are defined by Boolean algebra.	Operations are defined by linear algebra over Hilbert space.
Circuit behavior is defined by classical physics.	Circuit behavior is defined by quantum mechanics.

©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget

According to IBM, "Groups of qubits in superposition can create complex, multidimensional computational spaces," which enables more complex computations. When qubits become entangled, changes to one qubit directly affect the other, which makes information transfer between qubits much faster.

In classical computers, algorithms need a lot of parallel computations to solve problems. Quantum computers can account for multiple outcomes when they analyze data with a large set of constraints. The outputs have an associated probability, and quantum computers can perform more difficult compute tasks than classical computers can.

Power of classical vs. quantum computers

Most classical computers operate on Boolean logic and algebra, and power increases linearly with the number of transistors in the system -- the 1s and 0s. The direct relationship means in a classical computer, power increases 1:1 in tandem with the transistors in the system.

Because quantum computers' qubits can represent a 1 and 0 at the same time, a quantum computer's power increases exponentially in relation to the number of qubits. Because of superposition, the number of computations a quantum computer could take is 2^N where N is the number of qubits.

Operating environments

Classical computers are well-suited for everyday use and normal conditions. Consider something as simple as a standard laptop. Most people can take their computer out of their briefcase and use it in an air-conditioned café or on the porch during a sunny summer day. In these environments, performance won't take a hit for normal uses like web browsing and sending emails over short periods of time.

Data centers and larger computing systems are more complex and sensitive to temperature, but still operate within what most people would consider "reasonable" temperatures, such as room temperature. For example, ASHRAE recommends A1 to A4 class hardware stays at 18 to 27 degrees Celsius, or 64.4 to 80.6 degrees Fahrenheit.

Some quantum computers, however, need to reside in heavily regulated and stringent physical environments. Some need to be kept at absolute zero, which is around -273.15 degrees Celsius or -459.67 Fahrenheit, although recently the first room-temperature computer was developed by Quantum Brilliance.

The reason for the cold operating environments is that qubits are extremely sensitive to mechanical and thermal influences. Disturbances can cause the atoms to lose their quantum coherence -- essentially, the ability for the qubit to represent both a 1 and a 0 -- which can cause errors to computations.

Why data center managers should take note of quantum computing

Like most technologies, quantum computing poses opportunities and risks. While it might be a while before quantum computers really take off, start to have conversations with leadership and develop plans for quantum computing.

Organizations that don't plan on implementing quantum computing in their own business will still need to prepare for the external threats quantum computing might impose. Firstly, quantum computers can potentially crack even the most powerful and advanced security measures. For example, a motivated enough hacker can, in theory, use quantum computing to quickly break the cryptographic keys commonly used in encryption if they are savvy.

In addition, organizations that are considering quantum computers for their data centers or certain applications will have to prepare facilities. Like any other piece of infrastructure, quantum computers need space, electricity supply and resources to operate. Begin examining the options available to accommodate for them. Look at budget, space, facility and staffing needs to begin planning.

19.Post-Quantum Cryptography Experts Brace For Long Transition Despite White House Deadlines

by Dave Nyczepir
https://www.fedscoop.com/quantum-crytography-experts-long-transition/

The White House's aggressive deadlines for agencies to develop post-quantum cryptography strategies make the U.S. the global leader on protection, but the transition will take at least a decade, experts say.

Canada led the Western world in considering a switch to post-quantum cryptography (PQC) prior to the Office of Management and Budget issuing its benchmark-setting memo on Nov. 18, which has agencies running to next-generation encryption companies with questions about next steps.

The memo gives agencies until May 4, 2023, to submit their first cryptographic system inventories identifying vulnerable systems, but they'll find the number of systems reliant on public-key encryption — which experts predict forthcoming quantum computers will crack with ease — is in the hundreds or thousands. Agencies, software, servers and switches often have their own cryptography, and agencies don't necessarily have the technical expertise on staff to understand the underlying math.

"This will be the largest upgrade cycle in all human history because every single device, 27 billion devices, every network and communication needs to upgrade to post-quantum resilience," Skip Sanzeri, chief operating officer at quantum security-as-a-service company QuSecure, told FedScoop. "So it's a massive upgrade, and we have to do it because these quantum systems should be online — we don't know exactly when — but early estimates are three, four years for something strong enough."

Bearish projections have the first quantum computer going live in about a decade, or never, with scientists still debating what the definition of a qubit — the quantum mechanical analogue to a bit — should even be.

QuSecure launched three years ago but became the first company to deploy PQC for the government this summer, when it proved to the U.S. Northern Command and North American Aerospace Defense Command that it could create a quantum channel for secure aerospace data transmissions at the Catalyst Campus in Colorado Springs, Colorado. The company used the CRYSTALS-KYBER cryptographic algorithm, one of four the National Institute of Standards and Technology announced it would standardize, but a quantum computer doesn't yet exist to truly test the security.

The first quantum security-as-a-service company to be awarded a Phase III contract by the Small Business Innovation Research program, QuSecure can contract with all federal agencies immediately. Customers already include the Army, Navy, Marines and Air Force, and the State, Agriculture, Treasury and Justice departments have inquired about services, Sanzeri said.

QuSecure isn't alone.

"We are having discussions right now with various federal agencies around what they should be doing, what they can be doing, in order to start today — whether it's in building out the network architecture or looking at Internet of Things devices that are being sent into the field," said Kaniah Konkoly-Thege, chief legal officer and senior vice president of government relations at Quantinuum, in an interview.

Defense and intelligence agencies are better funded and more familiar with classified programs requiring encryption services and therefore “probably in a much better position” to transition to PQC, Konkoly-Thege said.

Having served in the departments of the Interior and Energy, Konkoly-Thege said she’s “concerned” other agencies may struggle with migration.

“There are a lot of federal agencies that are underfunded and don’t have the resources, either in people or funding, to come and do what’s necessary,” she said. “And yet those agencies hold very important information.”

That information is already being exfiltrated in cyberattacks like the Office of Personnel Management hack in 2015, in which China aims to harvest now, decrypt later (HNDL) data with fully realized quantum computers.

Post-Quantum CEO Andersen Cheng coined the term, and his company’s joint NTS-KEM error-correcting code is in Round 4 of NIST’s PQC algorithm competition.

Cheng points to the fact he could trademark his company’s name as proof PQC wasn’t being taken seriously even in 2015 and certainly not the year prior, when he and two colleagues were the first to get a PQC algorithm to work in a real-world situation: a WhatsApp messaging application downloadable from the app store.

They took it down within 12 months.

“One of my friends in the intelligence world called me one day saying, ‘You’re very well known.’ I said, ‘Why?’ He said, ‘Well, your tool is the recommended tool by ISIS,’” Cheng told FedScoop in an interview. “It was a wonderful endorsement from the wrong party.”

While there wasn’t one moment that caused the U.S. government to take PQC seriously, Cheng said the “biggest” turning point was the release of National Security Memo-10 — which OMB’s latest memo serves as guidance for implementing — in May. That’s when the largest U.S. companies in network security infrastructure and finance began reaching out to Post-Quantum for consultation.

Post-Quantum now offers a portfolio of quantum-ready modules for not only secure messaging but identity, quorum sensing and key splitting.

Cheng said the Quantum Computing Cyber Preparedness Act, sent to President Biden’s desk Friday, should become law given PQC’s momentum, but he has “slight” reservations about the OMB memo’s aggressive deadlines for agencies to declare a migration lead and to conduct an inventory audit.

“People are probably underestimating the time it will take because the entire migration — I’ve spoken to some very top-end cryptographers like the head of crypto at Microsoft and so on — our consensus is this is a multi-year migration effort,” Cheng said. “It will take 10 years, at least, to migrate.”

That’s because public-key encryption protects everything from Zoom calls to cellphones, and the National Security Agency isn’t yet recommending hybridization, which would allow for interoperability among the various NIST-approved algorithms and also whichever ones other countries choose. Agencies and companies won’t want to swap PKE out for new PQC algorithms that won’t work with each other, Cheng said.

Complicating matters further, NIST is approving the math behind PQC algorithms, but the Internet Engineering Task Force generally winds up defining connectivity standards. Post-Quantum's hybrid PQ virtual private network is still being standardized by IETF, and only then can it be added to systems and sold to agencies.

Cheng recommends agencies not wait until their inventory audits are complete to begin talking to consultants and software vendors about transitioning their mission-critical systems because PQC expertise is in short supply. Large consulting firms have been "quietly" building out their quantum consulting arms for months, he said.

OMB's latest memo gives agencies 30 days after they submit their cryptographic system inventory to submit funding assessments, a sign it won't be an unfunded mandate, Sanzeri said.

"This is showing that all of federal will be well into the upgrade process, certainly within 12 months," he said.

20.The FBI Says Apple's New Encryption Is "Deeply Concerning"

by Maggie Harrison
https://futurism.com/the-byte/fbi-apple-new-encryption-deeply-concerning

Apple is planning on broadening its end-to-end data encryption services, closing a privacy loophole that previously allowed law enforcement to access a wide-reaching swath of data, including photos and messages, stored in user iCloud accounts.

But while proponents of the change are applauding the change as a win for user privacy, its detractors — which include a little organization known as the FBI — are none too thrilled.

The bureau is "deeply concerned" with the perceived "threat end-to-end and user-only-access encryption pose," as they wrote in an email to *The Washington Post*, basically arguing that the tech makes their jobs a lot harder.

"This hinders our ability to protect the American people from criminal acts ranging from cyber-attacks and violence against children to drug trafficking, organized crime and terrorism," the statement continued, according to *WaPo*. "In this age of cybersecurity and demands for 'security by design,' the FBI and law enforcement partners need 'lawful access by design.'"

Trade-Offs

In short, the FBI's argument rests on the notion that, just like they can search someone's physical stuff, they should be able — within reason — to search their digital stuff, too.

That being said, while the FBI's concerns make sense, end-to-end encryption isn't just an Apple plot to piss the agency off, nor is it intended to make doing crimes any easier. User privacy is important, and a lot of folks have spent the better part of a decade giving away a *lot* of data, often without much agency or understanding. Data breaches and hacking incidents, meanwhile, are common. The new end-to-end encryption — which, *The New York Times* points out points out, won't be expanded to include Apples' email, calendar, or contacts features — would certainly bolster user security.

All to say: when it comes to data encryption, tech companies, law enforcement agencies, and users themselves have yet to find a solution where everyone wins.

"It's great to see companies prioritizing security," Sasha O'Connell, executive in residence at American University and former FBI section chief, told the *NYT,* "but we have to keep in mind that there are trade-offs." Speaking to the *NYT*, O'Connell made another interesting point, offering that, at the end of the day, the final choice appears to be Apple's, and Apple's alone.

"The big question is: Who decides that trade-off?" she continued. "It continues to sit in Apple's hands."

21.Preparations For Quantum Cyber Threat Get A Senate Boost

by Mariam Baksh
https://www.nextgov.com/cybersecurity/2022/12/preparations-quantum-cyber-threat-get-senate-boost/380698/

Four lawmakers praised Senate passage of their bill to protect sensitive information from the prospect of a quantum computer capable of decoding current cryptographic standards, supporting the Biden-Harris administration's plan to address such a threat.

Quantum computers with the ability to decipher present-day encryption with faster-than-ever calculation power are still considered to be a decade or more away. But supporters of the administration's plan say adversaries could be harvesting data now with the intention of decrypting it in the future, once they've sufficiently developed the nascent technology.

"Data breaches exploited by quantum computing are a serious national security concern," Sen. Maggie Hassan, D-N.H., said in a press release Friday. "America's adversaries look for any vulnerabilities in our cybersecurity systems in order to threaten our infrastructure, data and security. It is crucial that we are ready to defend against any adversaries using this incredibly sophisticated and emerging technology against our country. Protecting our homeland security is a bipartisan issue—I am pleased that the Senate passed our bill and I'll keep working to get this across the finish line."

Hassan was joined by Sen. Rob Portman, R-Ohio, and Reps. Ro Khanna, D- Calif., and Nancy Mace, R-SC., in praising the Senate's passage of the House version of the bill Thursday.

The Quantum Computing Cybersecurity Preparedness Act largely echoes a national security memo the administration issued in May laying out deadlines for agencies to inventory all currently deployed cryptographic systems in order to prioritize their transition to forms of encryption experts say would be invulnerable to speedy quantum computers.

The National Institute of Standards and Technology and the National Security Agency are currently developing standards for the implementation of four quantum-resistant algorithms NIST announced in July after inviting scientists around the world to submit their proposals. In anticipation of the algorithms, a January national security memo granted NSA the power to issue binding operational directives to facilitate agencies' migration to the new standards.

In addition to reiterating the administration's instructions for agencies, including the Office of Management and Budget, the legislation directs OMB to report annually to Congress on the migration effort. The reports should outline the administration's strategy and projected costs, according to the press release.

"As quantum computing advances, we need to take steps to protect the personal data of Americans as well as U.S. national security and government agencies data," Khanna said. "I'm thrilled that the Senate has passed this bill to proactively keep our systems and valuable data safe and establish Congress' oversight role in the process."

22. Toshiba's 30 Years Of Research Pave The Way For Quantum-Safe Communications Links

by Toshiba
https://www.digiconasia.net/sponsored/toshibas-30-years-of-research-pave-the-way-for-quantum-safe-communications-links

Growing the quantum communications ecosystem in the region requires quantum cryptography over vast distances.

From the secure transmission of sensitive genomic data, to data transfers between critical industrial infrastructure, to the day-to-day exchange of personally-identifiable data in financial and healthcare sectors — digital communications are the lifeblood of critical human enterprise.

Despite the use of advanced cryptographic methods to ensure safe data exchange, the world is at the cusp of an age in which quantum computers that are magnitudes faster than today's supercomputers will be able to crack the best encryption schemes within practicable timeframes.

In anticipation of the arrival of accessible quantum computing resources, cybercriminals are already stealing (or 'eavesdropping') and hoarding sensitive information even when they cannot decrypt it. The idea is that the value of the information will be unleashed in the near future when these threat actors — presumably state-sponsored — will be able to decode the stolen data.

QKD in fiber and soon, satellite communications

Way back in 2003, Toshiba Corporation was already cognizant of the potential of quantum computing and its potential for both innovation and for abuse by the powers that be. The multinational conglomerate spearheaded quantum cryptography research at the Cambridge Research Laboratory and subsequently became the first technology firm to announce Quantum Key Distribution (QKD) capabilities of over 100 kilometers of fiber, and the first to achieve a continuous key rate exceeding 1Mbps in 2010, followed by 10Mbps in 2017. (Read more about Toshiba's QKD innovations here)

While QKD will keep quantum-empowered cybercriminals and state-sponsored threat actors at bay, the practical challenge is to facilitate such encryption over even longer distances, especially across rural areas. The natural answer to this challenge is satellite communications technology.

In that vein, a Singapore quantum communications firm, SpeQtral, has tapped into Toshiba's proven terrestrial QKD solution to facilitate transmission of quantum-encrypted data from Singapore to Europe via the upcoming SpeQtral-1 satellite in 2024.

On 16 November 2022, SpeQtral hosted a launch event of Quantum Networks Experience Center (QNEX) to showcase the fruits of its labor with longtime partner Toshiba. The experience center features multimedia exhibits that help laypeople to understand how quantum computing and QKD work, and also houses an actual QKD link between two secure data servers simulating real Sender and Receiver terminals sited far apart on earth. Also, the QNEX exhibits do better at explaining the intricacies of how to apply state-of-the-art technologies to scale down a bulky quantum encryption device to a size small enough to fit into a communications satellite.

Launch event messages

At the QNEX inauguration, the President & CEO of Toshiba Digital Solutions Corporation, Shunsuke Okada, announced: “QNEX is an important initiative that aims to raise awareness and understanding among governments and businesses in the region around how quantum cryptographic solutions can safeguard sensitive data and vulnerable infrastructures against present and future threats. We are happy to be part of this important initiative and look forward to working alongside SpeQtral to grow the QNEX partnership network in Singapore and the Southeast Asia region.”

SpeQtral’s CEO, Lum Chune Yang, noted: “Secure communications are foundational to establishing the complex ‘web of trust’ between buyers, sellers, and intermediaries in the modern digital economy. With this web under threat given advances in both traditional and quantum computing technologies, organizations will have to fundamentally change how they secure their most sensitive data. SpeQtral is on a mission to leverage advances in Quantum Cryptography and satellite technologies to build the world’s first global quantum-safe communication network… QNEX represents both Toshiba and SpeQtral’s commitment to support the awareness and adoption of the technology in Singapore and the broader Southeast Asian region.”

At the diplomatic level, Japan’s Ambassador to Singapore, His Excellency Hiroshi Ishikawa, commented: “Japan has initiated a new national strategy for quantum technology to create growth opportunities and social transformation including solving social issues. Singapore, in particular, is one of the global Innovation hubs. We are proud that SpeQtral and Toshiba will combine Singapore and Japan technologies to build a quantum-secured communication network to deal with security threats. The Japanese government will continue to provide the necessary support to strengthen the Japan-Singapore relationship.”

The QKD road (and satellite reach) ahead

Having invested billions into quantum and quantum cryptography research well before other firms, Toshiba’s 30 illustrious years of effort have now facilitated national research institutions and private startups alike to step out of Proof-of-Concept stages and into practical applications in Singapore and beyond.

Government and financial sectors are most likely to be early adopters of QKD solutions for quantum-safe communications networks. This is evident from the Singapore government’s long-term interest in supporting quantum technologies and quantum industrialization. Also, Singapore is a major global financial hub and offers strong market potential for QKD both in South-east Asia and around the world.

The Guest of Honour for the event, Deputy Prime Minister of Singapore and Coordinating Minister for Economic Policies, Heng Swee Keat, who is also Chairman of the National Research Foundation said:

“Over the last two decades, Singapore has invested in and built up capabilities in quantum technologies. In the coming years, as the use of digital technologies becomes more pervasive, the ability to safeguard and exchange data securely across the world will be even more critical. We will continue to invest in the National Quantum-Safe Network, a national research program that aims to advance quantum-safe communications and develop use cases. At the same time, we are building local and international partnerships. This latest collaboration between SpeQtral and Toshiba brings together the expertise of both parties to enhance the resilience of global and regional communications networks."

With innovative technologies like QKD and a deep commitment to a greener, better world, Toshiba is working towards more secure and stable data and energy infrastructures in Southeast Asia.

23.Meeting The Security Demands Of Post-Quantum Computing

by Kerry Doyle With Chung Hyun-Chul
https://www.lightreading.com/meeting-security-demands-of-post-quantum-computing/a/d-id/782186?

The South Korean company Norma is a leader in IoT and Quantum security. Established in 2011, the company provides expertise and network security solutions for a range of wired/wireless environments, from smart homes and smart cities to national grids and heavy industry. Post-quantum cryptography is crucial to defend against cyberattacks that are specifically targeting today's data. We spoke recently with Chung Hyun-chul, CEO of Norma to address critical post-quantum security issues.

As quantum computers become a reality, they will be able to break today's public-key cryptographic (PKC) security. What are some key steps that organizational leaders should take today to prepare and protect their organizations' data and systems?

The first thing to do is to figure out what public key cryptography (for example, RSA, ECC, etc.) is currently being used internally. Afterward, a roadmap planning on how to build a security system in response to the threat of quantum computers is required. Among many tasks such as network infrastructure, applications, and security solutions, it is highly recommended to prepare a roadmap strategy being appropriate for the characteristics of the respective enterprises, which should be prioritized and how to be converted.

Specifically, these are like performing a post-quantum risk assessment, diagnosing an organizational infrastructure, possessing a Crypto-Agility to respond to quantum attacks, checking how fast PKI can be migrated into post-quantum cryptography, adopting a hybrid method of PQC and classic cipher solutions, and designing a quantum-safe infrastructure, etc. These factors need to be taken into consideration comprehensively.

Cybercriminals use harvest now, decrypt later (HNDL) attacks to take advantage of quantum computers when they become more widely available. What can businesses do now to formulate their responses to HNDL, assess their security and prevent these attacks from potentially compromising their data?

That's a very good question. Quantum computers are not yet universal, but I think this is a very appropriate question to explain why businesses need to be proactive about quantum security. HNDL refers to the act of stealing encrypted current data with the expectation that if quantum computers are commercialized, public key cryptography can be broken.

Attackers can collect data without having the skills to decrypt it right now. However, when quantum computers are introduced in the near future, it will be possible for them to break cryptography and obtain information. This means that all data today is at risk of being hacked, and it is important to be aware that if not protected now, it could be disclosed at any time.

For example, if an attacker attempts to steal data based on HNDL, it will be a threat to disrupt national safety nets, from smart cities, autonomous vehicles, and corporate industrial operations to power plants, financial data and security intelligence.

So, before discussing how to transform a system, businesses must assume that their encrypted data is potentially decryptable. On the premise of this factor, the corresponding scenarios and roadmaps should be prepared.

In this respect, the step-by-step roadmap needs to be arranged. Since a full-scale transition to quantum security is expensive, a sequential approach is required by securing important information or infrastructure in advance.

Crypto-Agility combines current, tested cryptography like RSA with post-quantum algorithms. How important is it and what are the advantages for companies to work with partners that practice hybridization and Crypto-Agility?

As mentioned earlier, preparing a secured system for a quantum computer requires a lot of investment in terms of time and money. It also requires high security skills.

However, changes to cryptographic operations should not affect functionality, and users should not feel uncomfortable or alienated from the system changes. A company's concerns about Crypto-Agility can be addressed with the consultation and solutions from the companies specializing in cryptographic security.

Accordingly, the collaboration with a professional security firm brings economic benefits to the company by reducing trial and error through the technology and know-how of a professional security firm with various experiences, reducing costs and increasing efficiency.

Decision-makers can pursue one of three paths: adopt post-quantum cryptography (PQC) solutions today, retrofit existing systems to PQC standards or significantly enhance their traditional encryption protocols. Could you discuss some of drawbacks and trade-offs to consider for each approach?

Well, among three options, the first is to adopt a PQC environment across the infrastructure, including solutions such as applications from the beginning. The second is to change only the system's ciphers to the PQC standard, and the third is to modify the algorithm, like increasing the key length, or taking additional security measurement on to the current system.

Of course, adopting the first PQC solution is the most ideal and an ultimate alternative, but it may be difficult to make a full-scale conversion right away because it requires a lot of investment in terms of time and money. In addition, since it is a new technology that has not been tested on the market yet, there may be risks in terms of safety.

The second option can lead to unexpected issues in terms of compatibility between legacy systems and ciphers, resulting in additional costs. And each revision will eventually have the same effect of adopting a full-fledged PQC environment. So, it's a good idea to plan it well from the beginning and move forward step by step to the first option.

The third option is difficult to choose, especially because it has problems that require a lot of resources, such as speed and memory, and is not a fundamental solution.

For companies developing solutions with the PQC technology applied, it is recommended to use the existing system and the new solution in parallel by preparing a strategy with the help of a professional consulting firm. Relatively low-importance, or costly work can be managed with the existing system, and the new PQC technology can be applied to the core systems and sensitive data only, expanding the application gradually.

What is the difference between QKD and PQC technology and application, and what is the current global trend?

Quantum cryptography is largely divided into QKD, quantum cryptography key distribution with the hardware chip applied and PQC which is a software-based post-quantum cryptography. QKD is a quantum cryptography, which theoretically guarantees very high security, but it requires high costs, various conditions and additional infrastructure for its implementation. Therefore, it is quite difficult to introduce QKD into the market in a fast manner. On the other hand, PQC is a cryptographic technology based on mathematical problems that quantum computers take too much time to solve. It can be applied to the infrastructure by replacing the existing cryptograph-ic algorithms without the need for special equipment. In particular, it can be applied only by software implementation, so its scope is relatively wide.

Due to these characteristics, QKD-centered discussion was conducted in the early days of quantum security, but now PQC is attracting attention for technical reasons, and it is expected that PQC will take up a much larger share in the future.

Today, Norma is accelerating the commercialization of PQC in partnership with several large cor-porations and public institutions in Korea. We are carrying out pilot projects with HDC (Hyundai Development Company) and SK Telecom. Now we plan to expand the collaborations with global companies continuously in the future.

24.New Year's Resolutions For CIO

by John Roese
https://www.technologyreview.com/2022/12/07/1064486/new-years-resolutions-for-cios/

From security to quantum, AI and edge to cloud, our digital world is evolving and expanding more quickly than ever. With so much “noise,” it can be hard to concentrate, let alone figure out where to start beyond the bits and bytes, speeds and feeds. I hear this from everyone I meet with, and it’s clear that CIOs, in particular, are feeling the pressure. So this year, I’m going to outline four emerging technologies and describe how CIOs can take action on them today. Consider these your new year’s resolutions.

1. **I will not use cloud without understanding the long-term costs.** I’ve been hearing from CIOs that their initial eagerness to take advantage of cloud computing has put them over budget, as they weren’t thinking strategically about how to distribute IT capabilities across different cloud providers—let alone how to make them work together. My recommendation is to both characterize the technical viability of running a workload or placing data into a specific cloud, and also fully identify the short- and long-term costs of using that cloud. If you know going in what the costs are, you can better target workloads to the right long-term home. This will also set you up to evaluate new cloud options and find potential cost reductions over time.

2. **I will define my zero-trust control plane.** We will continue to see an increase in industries requiring zero-trust frameworks, such as those set forth by the U.S. government. These requirements will have a global ripple effect across critical infrastructure industries. So where do you begin? You need to

have an authoritative identity management, policy management, and threat management framework to do zero trust properly. And if you don't have a well-defined and authoritative control plane over your multi-cloud environment, how can you possibly achieve consistent identity, policy, or threat management for your total enterprise? Security in the multi-cloud, more than any other aspect, needs to be consistent and common. Silos are the enemy of real zero-trust security.

3. A. **I will establish early skill sets to take advantage of quantum.** Quantum computing is getting real, and if you don't have someone in your business who understands how this technology works and how it influences your business, you will miss this technology wave. Identify the team, tools, and tasks you'll devote to quantum and start experimenting. Just last month we announced the on-premises Dell Quantum Computing Solution, which enables organizations across industries to begin taking advantage of accelerated compute through quantum technology otherwise not available to them today. Investing in quantum simulation and enabling your data science and AI teams to learn the new languages and capability of quantum is critical in 2023.

3. B. **I will determine where my quantum-safe cryptography risks lie.** Quantum computing is so disruptive because it changes many elements of modern IT. With the rise of quantum computing comes the need to better understand post-quantum cryptography, the development of cryptographic systems for classical computers that are able to prevent attacks launched by quantum computers. Bad actors globally are actively trying to capture and archive encrypted traffic on the assumption that sufficiently powerful quantum computers will eventually be able to decrypt that data.

   Want to mitigate your risk? I suggest starting with understanding where your biggest risk exists—as well as the time horizon you are worried about. You can do this by first cataloging your crypto assets and then identifying which encrypted data is most exposed to public networks and possible capture. That is the first place you need post-quantum cryptography. In 2022, NIST selected the first few viable post-quantum algorithms, and in 2023 these tools will start to emerge. Over time they will be needed everywhere, but in 2023, knowing where to use them first is a critical step.

4. **I will decide whether my multi-cloud edge architecture needs to be cloud extension or cloud-first.** In 2023 more of your data and processing will be needed in the real world. From processing real-time data in factories to powering robot control systems, edge is expanding rapidly in the multi-cloud world. This year you will need to make a choice about which edge architecture you want long term.

   Option one is to treat edges as extension of your clouds. In that common model, for each cloud you have an equivalent edge (for example, GPCP-Anthos, Azure-ARC, AWS-EKS). This works well if you only have one or a few clouds. Option two is to treat your edge as a platform for all your clouds to share. This edge-first architecture is new but with efforts like Project Frontier, we are seeing a path to build out a stable shared edge platform that can be used by any software-defined edge (for example, ARC, Anthos, EKS, IoT apps, or data management tools). Though multi-cloud edge platforms are just emerging, it's critical to make a decision now about what you want your edge to look like in the future. Do you want a proliferation of edges for each cloud service you use or do you want those cloud services to be delivered as software on a common platform?

Hopefully these four resolutions will make all of us better prepared for the multi-cloud future. Innovation has never been as pervasive and fast moving as we expect in 2023, which increases the urgency to make forward-looking decisions that will help us navigate the technology stream coming at us.

25.FSR Outlook 2023: Get Ready For The Quantum Leap

by Karen Anderson, Nayan Bhathela and Jaime de San Román

https://www.lexology.com/library/detail.aspx?g=988c2293-d70c-42cb-a089-bbcaec07ed3a

Quantum computing is set to reshape financial services. We explore the risks and opportunities inherent in this cutting-edge technology.

Broadly speaking, quantum computers operate as follows:

- Quantum computing uses quantum bits (qubits), which are atomic or subatomic objects (eg, photons or electrons) that have both wave- and particle-like physical properties. Unlike bits used in classical computers that exist in only one state of 0 or 1, qubits exist in more than one state at the same time – this is known as superposition.
- Qubits can only exist in a superposition of values until they are measured, at which point they collapse and immediately revert to a value of either 0 or 1. The state of superposition is very fragile, and one of the key challenges in developing a functional quantum computer is to eliminate all sources of noise and errors which could result in such collapse.
- When qubits are be linked on the quantum level (which is known as entanglement), their values are correlated such that measurement of one qubit instantly affects the other entangled qubits. By encoding data into entangled qubits and performing operations which leverage quantum theory on those qubits, in mere hours we can, with quantum computers, solve problems that would take a classic computer or super-computer tens of thousands of years. However, as the number of entangled qubits on a quantum computing processor increase, so does the difficulty in maintaining their fragile states.

Researchers have recently made some significant breakthroughs in addressing these issues including (to name but a few): in 2019, Google's quantum computer was reportedly the first to perform a calculation that would be practically impossible for a classical computer ("quantum advantage"); in June 2022, Australia's Silicon Quantum Computing created the first integrated circuit manufactured at atomic scale; in August 2022, Quantinuum found a way to scale the number of qubits to increase performance and reduce the error rate; and in October 2022, researchers from China, the UK and the US devised a temperature control technique to keep qubits stable for longer. All this is still really "laying the groundwork" for more complex computations that might eventually solve industry-relevant problems. Nonetheless, the pace is picking up - IBM envisages that delivery of its new quantum system in 2023 will prove to be an inflection point after which the errors of quantum computing will decrease exponentially; Google aims to have a commercial grade quantum computer by 2029.

The opportunities

In the short term, the resources involved in obtaining access to and operating quantum computers will likely only be justified for a relatively small group of problems. However, for those particular problems, which for financial services would include addressing the difficulty classical computers have in factoring large numbers, and searching large datasets such as unordered lists, quantum computing could be a game-changer. It is also likely to involve the use of quantum-as-a-service providers (such as Microsoft's Azure Quantum or D-Wave's Advantage) in the short to medium term.

Potential uses of quantum computing for financial institutions include optimisation of trading algorithms, risk profiling and management, enhanced compliance operations and detection of financial crime, customer targeting and prediction. The Monetary Authority of Singapore is supporting a research project which aims to develop quantum computing based credit scoring methods for trade finance. IBM has even posited that quantum computing could forecast financial crashes. First movers such as JP Morgan, Goldman Sachs, BBVA and Santander (amongst others) have established quantum research teams who use experimental systems to explore potential use cases such as portfolio optimisation, speeding up derivatives pricing, simulation and machine learning.

Regulators are beginning to focus on these issues. The UK's FCA held a virtual workshop with a range of stakeholders to consider the possible impacts of quantum computing for security and encryption, and competition in financial services, amongst other policy considerations. Other regulators, including Singapore's MAS, the French AMF, Germany's BaFin, Hong Kong's HKMA, and Canada's OSFI, have alluded to the risks quantum computing may pose for blockchain applications and many widely used security procedures.

In the US, the National Institute of Standards and Technology (NIST) (a public/private collaboration) has been working on developing a post-quantum cryptographic standard – four algorithms have been selected for standardisation and the standards are expected to be published by 2024; work on digital signatures algorithms is ongoing. NIST has urged firms to start preparing for the migration to post-quantum cryptography now: “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”. The European Telecommunication Standards Institute has separately proposed a three-stage action framework for migration to such standards.

A number of larger banks have already started work on what will likely prove to be a very long term transformation project. Typically, such projects start with the formation of an expert team, and an audit of current operating systems, network services and applications, to identify and inventory where and how high-risk data is held. Hardware and software encryption protocols currently in use are assessed, taking into account their purpose, to identify those which are vulnerable to quantum computers, with a view to prioritising them for future-proofing so that work on adopting relevant standards can begin as soon as these are available. Financial services firms should also start including in all future projects consideration of the quantum-related risks and any steps that will be eventually be required to transition them to quantum-safe protocols.

As the FCA noted, "it is critical that all parts of the financial services sector start collaborating now to ensure this is a quantum leap for the better and not a stumble into the unknown”.

26.Zapata Computing Earns 2 New Patents For Post-Quantum Cybersecurity Threat Intelligence

by Zapata Computing
https://www.hpcwire.com/off-the-wire/zapata-computing-earns-2-new-patents-for-post-quantum-cybersecurity-threat-intelligence/

Zapata Computing, a leading enterprise quantum software company, today announced that the company has earned two new patents for post-quantum cybersecurity techniques. The new patents are for its **Variational Quantum Factoring (VQF)** and **Quantum-Assisted Defense Against Adversarial AI (QDAI)** algorithms.

With the addition of these patents, Zapata now owns one of the world’s largest quantum computing software patent portfolios. The company’s growing portfolio includes a diverse range of proprietary quantum algorithms, machine learning, optimization and hardware methods.

VQF and QDAI In the Age of Post-Quantum Cybersecurity Threat Intelligence

As the narrative regarding post-quantum cybersecurity continues to gain momentum across the security, intelligence and technology landscapes, VQF and QDAI underpin Zapata's post-quantum cybersecurity threat intelligence solutions for its customers.

VQF is a heuristic algorithm for cryptanalysis that can run on near-term quantum devices, quantum-inspired data structures, and other special purpose classical hardware. The hybrid quantum-classical algorithm was developed by Zapata's technical experts and is a technique that demonstrates that an adversary can already start attempting to compromise existing encryption schemes using heuristic algorithms. A heuristic algorithm is designed to solve a problem faster than traditional methods by sacrificing accuracy or completeness for speed. This means that VQF is effective at identifying specific instances of the encryption vulnerability – helping enterprises shore up defenses in advance of an attack.

"VQF introduces a new category of decryption possibilities that could arrive a lot sooner than the market expects," said Yudong Cao, CTO and co-founder of Zapata Computing. "We don't need to wait for a fully fault-tolerant computer that can run Shor's algorithm to see the threat. It's not a sudden 'one-day' jump. VQF demonstrates that an adversary can try to compromise existing encryption schemes using heuristic algorithms that don't have a mathematically provable guarantee they will compromise all instances. Using Shor's algorithm, factoring a 2048-bit RSA number requires a quantum computer with millions of physical qubits running for hours. We estimate that VQF can factor a 2048-bit RSA number with approximately several thousand NISQ qubits in around the same amount of time."

QDAI is the first hybrid quantum-classical algorithm for defense against adversarial attacks. Machine learning (ML) classification models are prone to adversarial attacks. These attacks add a very small — but carefully chosen — variance to data that confuses the classifier, rendering results to be incorrect. Quantum computers provide a new method of attack against ML models that possess a uniquely quantum noise meant to confuse the model. QDAI trains ML models to be immune to these types of adversarial AI attacks.

"Quantum computers have a high potential to exploit potential vulnerabilities of neural networks," added Cao. "As threats accumulate and adversarial AI models get stronger, we must leverage the power of quantum and classical resources to successfully defend against these attacks. That's exactly the reason we developed QDAI. As quantum computers grow, we may be able to switch to a fully quantum classifier, but in the meantime, there is potential for significant gains with the quantum-classical hybrid approach like QDAI."

"Zapata is consistently pushing the innovation envelope, developing new proprietary methods and technology that can benefit our customers and the ecosystem," said Christopher Savoie, CEO of Zapata Computing. "These patents represent a growing focus and concern regarding the threat that quantum computers present to national security and global enterprises. We developed VQF and QDAI as proactive threat intelligence techniques in order to develop countermeasures so our enterprise and government customers can assess their systems and make them more robust against an attack. We anticipate that more vulnerabilities will emerge as quantum and AI technology mature, and we'll continue to research and identify new threats down the road to try to stay a step ahead."

27.Preparing Cryptography For The Risks Of A Post-Quantum Computing World

by Joppe Bos
https://www.electronicdesign.com/technologies/embedded-revolution/article/21255911/nxp-semiconductors-preparing-cryptography-for-the-risks-of-a-postquantum-computing-world

Feeling happy about the security of your systems, data, and online banking? That's good because, today, we don't have the computing performance available to break the cryptography that protects it. Well, to clarify, not in a reasonable amount of time orat an affordable price. But change is on the way.

Thanks to intense research into quantum computing, machines could be available in as little as 10 years that are able to extract your cryptographic keys in the blink of an eye—at least in comparison to the efforts required with today's technology. Luckily, the security community has been working to find new algorithms that will be secure in a post-quantum computing age.

What's Been Keeping Our Digital Systems Safe?

Cryptography relies on mathematical functions that are easy to compute in one direction (e.g., the multiplication of two large numbers) but exceptionally challenging to reverse (given a large number, find the two numbers that were multiplied to get this result). This means that website visits, bank payments, and access to encrypted data are easy for you, but hard for those looking to break into those systems.

In fact, because today's cryptography is so good, hackers frequently resort to social engineering to acquire passwords and two-factor authentication pins rather than brute force the keys that protect data.

However, the core premise of this security is that it's too costly to build a machine that could break it and/or it would take far too long to execute. Consequently, we no longer use the symmetric key cipher DES, the Data Encryption Standard, standardized in the late 1970s.

At the time, Whitfield Diffie and Martin Hellman determined a machine costing $20M would be needed to brute force the standard in around 12 hours. By the late 1990s, a custom DES-cracker costing $250k broke a DES key in two days, with another $10k machine repeating the feat in 24 hours in 2006.

Now, in 2022, researchers from IBM and Google to D-Wave and TU Delft (Delft University of Technology, Netherlands) regularly announce improvements to their quantum computers. While these machines will deliver significant advances to society, their ability to rapidly perform integer factorization is a concern since this is the math that underpins much of today's public-key infrastructure. In a nutshell, today's public-key cryptography can be considered broken when facing the computational power of a quantum computer.

Searching for Post-Quantum Cryptographic Algorithms

After it became clear that DES was no longer fit for purpose, the National Institute of Standards and Technology (NIST), a physical sciences laboratory and non-regulatory agency of the U.S. Department of Commerce, set out to find alternatives. In response to a contest organized by NIST, the Advanced Encryption Standard (AES) was selected as the replacement in 2001.

With the security of current cryptography again at risk, NIST started a new contest to find suitable public-key post-quantum cryptographic (PQC) algorithms in 2016 to replace the existing RSA and elliptic-curve cryptography (ECC) standards.

When AES was selected, the internet was new and massive connectivity, such as the Internet of Things (IoT), didn't exist. Today, the systems demanding security are much more diverse, causing significant challenges for today's algorithm developers.

Not only must protection against quantum-computer attacks be assured, but it also must be possible to execute the encryption algorithm on today's small, performance-limited, low-power microcontrollers. Key size is another important way through which security can be improved. However, smart cards and IoT nodes may only provide kilobytes of storage, so this had to be considered.

Four PQC algorithms have been selected in the following six years, with more expected to be announced in the upcoming years. The first algorithm selected is CRYSTALS-Kyber, supporting comparatively small keys (compared to the other PQC candidates) and good operational speed. This is earmarked for the general key exchange used to protect data shared over public networks.

The other three are CRYSTALS-Dilithium, FALCON, and SPHINCS+, targeting the digital signatures used in authentication. Entries were submitted by teams from around the world, often combining industry and academia knowledge.

How PQC Algorithms Differ from Today's Cryptography

The CRYSTALS and FALCON algorithms rely on the hardness in solving the learning-with-errors (LWE) problem over module lattices. By comparison, SPHINCS+ is based on problems from the realm of cryptographic hash functions. While this algorithm is slower and results in larger code, its inclusion in the winning group of algorithms provides some mathematical diversification, should a weakness be found in the others.

Those who developed these algorithms believe that they will be secure against cyberattacks supported by quantum computers once machines with enough qubits exist.

For software developers, especially in the area of embedded systems, it must be noted that PQC algorithms are much slower due to the different math involved. NIST has considered algorithm execution as part of the selection process, and these algorithms are among the fastest and most secure options submitted.

Another aspect is key size. Using RSA, highest security is attained with keys of 3,000 to 4,000 bits, while ECC requires much less at 32 to 64 bytes. Our new PQC algorithms will need keys of several kilobytes, placing semiconductor vendors under pressure as they build the next generation of security hardware. However, it should be noted that some submissions demanded keys requiring well over 1 MB, so, again, we've got the best of the bunch.

Another concern is execution performance on embedded processors and the associated runtime memory requirements. Thanks to years of development and optimization, RSA and ECC are well understood and have a small footprint. Work has already started to evaluate PQC on processors such as the Arm Cortex-M4, a workhorse of embedded systems, with the open project "pqm4" available on GitHub.

CRYSTALS-Kyber proves to be amongst the fastest and most memory efficient. New accelerators and dedicated devices, such as secure elements (SE) and trusted platform modules (TPM), will undoubtedly be developed to further improve performance and keep power consumption under control.

The final concern is implementation. Those following the topic of embedded security will be aware of the extremes that researchers go to to discover design weaknesses. Power monitoring and RF analysis are just some approaches for finding side channels through which cryptographic implementations can be compromised.

Developers have learned much from these efforts and believe that the methods employed to protect ECC and AES hardware can be reused. However, to hedge their bets, new countermeasures also are being explored.

Transitioning to a Post-Quantum World

So, what can be done to prepare your security for a post-quantum world? Although the new PQC algorithms will not be standardized before 2024, there's plenty of preparatory work for businesses and organizations.

First, it makes sense to continue promoting good security practices amongst users of IT systems and mobile devices. Even PQC algorithms won't protect against phishing attacks. Today's most significant risk is that hackers go on a data-collection spree, stealing encrypted files and communication exchanges to deploy post-quantum computing to crack them in the years to come.

The second step is to clarify what security is implemented and where, especially for encrypted databases and files. One particular concern is the threat of store-now, decrypt later: Sensitive encrypted data could be stolen now and only decrypted when quantum computing becomes available.

Finally, developers can kick off exploratory conversations on PQC with vendors and suppliers to understand what will be available and when. Semiconductor vendors such as NXP, one of the contributors to CRYSTALS-Kyber, expect to have PQC-capable silicon available in the next few years, which will support the rollout and migration to this new worldwide security standard.

Cybersecure for the Years Ahead

Quantum computing is a real danger to the integrity of the security upon which we rely. While not yet advanced enough, it's clear that the math behind today's ECC and RSA algorithms will be no match for quantum computers.

Although it will take roughly two more years before we can see the new NIST PQC standards, those involved in cybersecurity, from cloud services and IT systems down to tiny IoT nodes, have concrete tasks to undertake. For some, just staying on top of developments will be enough so that, once solutions are available, they're ready to integrate them.

One thing is clear—we're ready for the post-quantum era. Thanks to the efforts of industry and researchers, our system and data security are assured.

28.The Truth About Wormholes And Quantum Computers

by Ethan Siegel
https://bigthink.com/starts-with-a-bang/wormholes-quantum-computers/

There should be one question you ask yourself anytime you encounter a claim that can be answered by science, “What is true?” Only by looking at the answer to that question — and, in particular, what can be and has been established to be scientifically true by the full suite of available evidence — can you draw a responsible conclusion. If we look at anything else, including what we hope, what we fear, or what unsupported speculations can’t be ruled out, we’re practically guaranteed to lead ourselves astray. After all, if the evidence isn’t enough to convince those with expert knowledge, it should be insufficient for the rest of us as well.

On November 30, 2022, a paper was published in Nature that claimed that a wormhole was simulated on a quantum computer, claiming that the observed features could be linked to real, traversable wormholes that could exist within our own Universe. There are three parts to this story:

1. the physics of wormholes within General Relativity,
2. the actual simulation conducted on a quantum computer,
3. and the link between our real Universe and the quantum computation,

and we have to get all three parts correct if we want to separate what’s true from the speculative, unsupported claims that many — including some of the study’s authors — have been publicly making. Let’s dive into all three.

The physics of wormholes

The idea of a wormhole was born very shortly after the discovery of the first exact, non-trivial solution in General Relativity: the Schwarzschild solution, corresponding to a non-rotating black hole. To obtain this solution, all you have to do is take completely flat, empty space and place down one object of infinitesimal volume, but finite mass. Wherever you place that down, you’ll have a black hole of a certain mass, surrounded by an event horizon of a specific radius determined by that mass. Einstein finished formulating General Relativity toward the end of the year in 1915, and in early 1916, Karl Schwarzschild published this early, remarkable solution that’s still relevant and widely-used today.

It was realized by a number of people — independently of one another — that if you were able to connect a Schwarzschild black hole (with a positive mass) at one location in the Universe to its negative mass/energy counterpart at another location, you could theoretically “bridge” those two locations. That bridge, in modern parlance, is now known as a wormhole. Originally, this theoretical solution was found by Flamm in 1916, then again by Weyl in 1928, and most famously once more by Einstein and Nathan Rosen in 1935.

Also known as Einstein-Rosen bridges, this early theoretical work paved the way for our modern understanding of wormholes within the context of General Relativity. While these early wormholes had a pathology to them in the sense that they would rip apart and destroy any matter that dared enter them, there have been a number of extensions that have been proposed to help “hold these wormholes open” as matter attempted to pass through it. We generally refer to this species of wormhole as a traversable wormhole, and most of the wormholes we encounter in science fiction are precisely of this flavor.

Whether or not wormholes can physically exist or not is a question that’s still hotly debated. Yes, we can mathematically write down solutions to Einstein’s equations that include them, but mathematics is not the same as physics. Mathematics tells you what’s within the realm of physical possibility, but only the actual, real Universe itself is going to reveal to you what’s physically true. The places we’d look for such physical evidence have all come up empty so far.

- We’ve observed real black holes; there are no signals from them suggesting they’re wormholes.
- We’ve observed lots of systems with positive energy; there are no systems with intrinsically negative energy.
- And we’ve observed lots of systems that possess three or fewer spatial dimensions; there’s yet to

be a shred of evidence for a fourth (or higher) spatial dimension.

The big dealbreaker for our Universe, as far as we know today, seems to be the lack of what one might call “exotic” matter. The simplest way of looking at the situation is to think of space as having an average energy density from all sources: matter, radiation, and even the (positive, non-zero) zero point energy of empty space itself. Where you have positive energy, space curves in response to that; this is why massive particles exhibit the phenomenon of gravitational attraction. So far, all we’ve ever detected in the Universe is matter-and-energy with positive values to it.

But if you want to have a traversable wormhole, you need some type of matter and/or energy that has a negative value to it, at least negative relative to the average energy density of the Universe. Although we can create small regions of space that have this property — e.g., the empty space between two parallel conducting plates, such as a setup exhibiting the Casimir effect — there are no species of negative energy quanta known to exist.

If they truly don’t exist at all, extra spatial dimensions, extra fields, or some sort of Planck-scale bridge (perhaps only allowing for the transfer of information, not matter) are the only ways that wormholes could physically arise within General Relativity.

The quantum simulation

In their recent paper, what the authors created was not an actual wormhole itself, but rather a quantum circuit that possesses some analogue behaviors and properties to a gravitational wormhole. This builds on earlier work, some of which needs to be recounted in order to understand the importance of this latest work.

Previously, some members of this team had concocted a scenario where a negative-energy pulse was transmitted between two topologically connected points, and that pulse was used for the purposes of quantum teleportation: to transfer the quantum state from one “side” of the two connected points to the other.

This is an interesting application, but it’s hard to see how it’s connected to wormholes and gravity. The only suggestion of a connection — and it’s important to emphasize that it’s only a suggestion — is that in 2013, Juan Maldacena and Leonard Susskind conjectured that a wormhole, or an Einstein-Rosen bridge, is equivalent to a pair of maximally entangled black holes. This connection is sometimes referred to as ER = EPR, to note that a wormhole (or Einstein-Rosen bridge) is connected to quantum entanglement, as the first paper on entanglement was authored by EPR: Einstein, Boris Podolsky, and Rosen.

We know that the full physical system is too difficult and complex to simulate with any sort of robust accuracy, so the authors did what practically all theoretical physicists do: they modeled a simpler approximation of the full problem, with the idea being that by simulating the simple approximation, many of the key properties of what would be a “true wormhole” would still persist. Partially because of the limitations of what we can actually simulate with current technology, and partially because of how limited human beings are in terms of the quality of models we can create, machine learning was used to design the experimental setup. According to Caltech’s Maria Spiropulu, coauthor of this paper:

“We employed learning techniques to find and prepare a simple [analogue] quantum system that could be encoded in the current quantum architectures and that would preserve the [needed] properties… we simplified the microscopic description of the [analogue] quantum system and studied the resulting effective model that we found on the quantum processor.”

The experiment showed that, once again, just as in the earlier experiment, quantum information traveled from one quantum system to the other: another example of quantum teleportation.

The link between the real Universe and this “quantum wormhole” simulation

Why should we care about this work, and what, if anything, does it teach us about the connection between wormholes and the types of simulations that a quantum computer can do?

The normally-sober Quanta magazine gave an accurate, in-depth account of the simulation performed on the quantum computer, but missed the boat entirely on this front, as many others were quick to correctly point out.

First off, the use of a quantum computer taught us nothing that we couldn’t learn (and didn’t already know in advance!) from using classical computers and hand calculations. In fact, the only novel thing that was accomplished by this team of researchers — a mix of quantum computation specialists and theoretical physicists — was that they were able to use machine learning to successfully simplify a previously complex problem into one that could be simulated using just a small number of qubits on a quantum computer. That’s an impressive technical achievement, and one that deserves to be celebrated for what it is.

But instead, many are celebrating this achievement for what it isn’t: evidence that wormholes have any relevance to our physical Universe, and/or evidence that this quantum simulation provides a window into how wormholes would actually behave in our Universe.

Here are some true things that you should know about what the newly-touted research actually did (and didn’t) do.

It did only use 9 qubits in their simulation. 9 qubits means that the quantum wavefunction encoded could at most require 512 (because 2^9 = 512) complex numbers to describe it, which is a simple enough wavefunction that it could be easily simulated on a classical computer. In fact, it was simulated on a classical computer by these very researchers *in advance* of the simulation they performed on their quantum computer! (With identical results to the limits of the quantum errors that arise from quantum computation processes in 2022.)

In other words, there was nothing that was learned from performing this simulation on a quantum computer other than the behaviors that they were expecting to see persisted even in this simple, 9 qubit simulation. Although this bodes well for future simulations along the same lines, it doesn’t provide any profound, fundamental insights beyond showing some potential for quantum computers.

So what about the connection to wormholes? You know, gravity-based wormholes within General Relativity that might actually apply to our real, physical Universe?

It’s about as speculative as it can get. First, it assumes that the holographic principle — which states that all physical properties within a volume of space can be encoded on a lower-dimensional boundary of that space — is, in fact, a property of the yet-undiscovered quantum theory of gravity. Second, instead of using the AdS/CFT correspondence, which is the established mathematical equivalence between a 5D anti-de Sitter space and the 4D conformal field theory that defines the boundary of that space, they use the suggestive correspondence between the Sachdev-Ye-Kitaev model and a two-dimensional anti-de Sitter space.

That’s a mouthful, but what that means is that they model gravity in “our Universe” as having one time dimension, one spatial dimension, and a negative cosmological constant, and then take what might be a mathematically equivalent description (the Sachdev-Ye-Kitaev model) and simulated that instead. Some of the properties they observed were analogous with some of the behaviors a traversable wormhole is expected to exhibit, but this provides no insights into how a traversable wormhole in our actual Universe, governed by General Relativity (in three spatial and one time dimension with a positive cosmological constant), would behave.

There are no lessons to be learned about quantum gravity here. There are no lessons to be learned about traversable wormholes or whether they exist within our Universe. There are not even any lessons to be learned about the uniqueness or capabilities of quantum computers, as everything that was done on the quantum computer can be done and had previously (without errors!) been done on a classical computer. The best that one can take away is that the researchers, after performing elaborate calculations of the Sachdev-Ye-Kitaev model through classical means, were able to perform an analogous calculation on a quantum computer that actually returned signal, not simply quantum noise.

But it's time to get real. If you want to study something relevant for our Universe, then use a framework that our Universe is actually analogous to. If you're only making an analogue system, be honest about the limitations of the analogue and the system; don't pretend it's the same as the thing you're oversimplifying. And don't lead people down the path of wishful thinking; this research will never lead to the creation of a real wormhole, nor does it suggest "wormholes exist" any more than spin-ice experiments suggest "magnetic monopoles exist."

Wormholes and quantum computers will likely both remain topics that are incredibly interesting to physicists, and further research into the Sachdev-Ye-Kitaev model will likely continue. But the connection between wormholes and quantum computers is virtually non-existent, and this research — despite the hype — changes absolutely nothing about that fact.

29.Post-Quantum Cryptography: What Is Emmanuel Macron Talking About?

by Louis Adam

https://www.lemonde.fr/en/pixels/article/2022/12/04/post-quantum-cryptography-what-is-emmanuel-macron-talking-about_6006537_13.html

The President of the Republic announced the sending of the 'first diplomatic telegram encrypted using post-quantum cryptography' to the French embassy in Washington. We explain its importance for the future of confidential communications.

"This tweet may sound technical – it is!" On Thursday, December 1, by announcing on Twitter that the first telegram encrypted using post-quantum technology had been sent, French President Emmanuel Macron was well aware that he would be referencing a topic unfamiliar to the general public. However, the development of post-quantum cryptography is of great importance to the world of cryptography, to confidential communications and, by extension, to the internet.

What is a quantum computer?

A quantum computer is not necessarily more "powerful" than a traditional computer. It is, however, better suited to solving certain problems that an ordinary machine would struggle with. One example is factoring: It is extremely difficult for a classical computer to decompose a number into prime factors, i.e. defining which prime numbers (numbers that can only be divided by themselves) it is the product of. For example, the factorization of 65 is 5 × 13, 5 and 13 being prime numbers.

In contrast, this task is easy for a quantum computer, a fact that has been known for nearly thirty years.

In 1994, the mathematician Peter Shor developed an algorithm capable of factoring large numbers using such a machine, which the American company IBM tested on a small scale in 2001.

In recent years, research on quantum computer projects has made significant progress. Several governments, like France, the United States and the United Kingdom, are funding major programs. Some large manufacturers, such as IBM, already have working quantum computers.

What does this have to do with cryptography?

The ability of the quantum computer to factorize has real consequences for the world of cryptography. The encryption algorithms used to ensure the confidentiality of data today are mainly based on certain mathematical functions. Among these are the calculation of the discrete logarithm... and the factorization of integers. The RSA algorithm – considered one of the bases of modern encryption – is based on the factorization of two integers.

Therefore, given that they have enough power, quantum computers could in theory easily break encryption and gain access to secret communications. To break the encryption of current algorithms by running Shor's algorithm, it's estimated that you would need a quantum computer with just over 1,000 qubits (the unit used to measure the computing power of quantum computers). In November, IBM announced that it had succeeded in producing a quantum computer capable of running 433 qubits, though it still has limitations. In the coming years, manufacturers are hoping to develop a quantum computer powerful enough to run Shor's algorithm.

What is the purpose of 'post-quantum cryptography?'

Anticipating this, the cryptography community has been working on new encryption algorithms that aren't reliant on operations vulnerable to quantum computers. These algorithms are referred to as "post-quantum cryptography."

In the United States, the National Institute of Standards and Technology has been running a program since 2016 to test and trial various proposed algorithms that are resistant to this threat. In July, after several "rounds," the institute presented the first four algorithms under consideration to become new standards in this area.

These proposals are a first step but remain experimental for now. As the French National Agency for Information Systems Security (ANSSI) noted in its official position on the subject, published in April, "it's important to recognize and take into account the immature nature of post-quantum cryptography: ANSSI will not approve any direct replacement in the short or medium term."

The agency is therefore calling for a certain amount of caution, while encouraging companies and organizations that use encryption to anticipate a possible replacement of algorithms in the years to come. This would be a major undertaking, not only involving a simple software update, but probably also the production and installation of dedicated devices in certain critical sectors, such as banking and the military.

What's in the telegram that Emmanuel Macron is talking about?

There's nothing particularly confidential about the content of the French diplomatic message mentioned by the President of the Republic. As explained in the Foreign Ministry's press release, it's a memorandum signed between the Minister of Higher Education and Research, Sylvie Retailleau, and Dr. Arati Prabhakar, Director of the US Office of Science and Technology Policy. This memorandum aims to support the joint efforts of France and the United States on quantum computing research.

The telegram primarily serves to highlight this issue, rather than signal that the French government actually putting post-quantum encryption tools into production. Nevertheless, companies are already trying to position themselves in light of this advance. French start-up

CryptoNext Security, which specializes in implementing new post-quantum encryption algorithms, carried out the encryption of this message sent across the Atlantic.

30.Taking The Best Path To Post-Quantum Security

https://www.lightreading.com/taking-best-path-to-post-quantum-security/a/d-id/782100

Quantum computing offers the potential to solve certain types of complex problems faster than classical computers by taking advantage of quantum mechanical effects. These quantum algorithms also have the ability to crack traditional cryptographic keys that protect today's data.

The threat potential has led to a rise in cases of harvest now, decrypt later (HNDL) attacks that could severely jeopardize personal data, destabilize the IT industry and threaten future security, impacting everything from smart cities and national grids to autonomous vehicles, industrial operations and financial markets. In this article, we look at the security issues at play with quantum computing and the benefits of collaborating with quantum experts and taking a software approach to post-quantum cryptography.

Ensuring future data protections

The trend toward quantum computing is well underway and while still highly experimental, mainstream adoption is inevitable. Research from Gartner indicates that in 2018, less than one percent of companies were budgeting to undertake quantum deployments. However, that figure is expected to increase to 20% by 2023[1]. The upward trend underlies the concern because quantum algorithms have the potential to recover the key of the currently used public key infrastructure (PKI).

Cybercriminals are threatening to take advantage of deficiencies in quantum security by disrupting national safety nets and using HNDL attacks to eventually decrypt the personal data of millions of users. Quantum computing also has the ability to crack traditional cryptographic keys that protect today's data.

In response, C-suite leaders need to consider a number of areas for post-quantum risk assessment that extend to infrastructure, networking and software. Their goal should be to immediately achieve robust data and infrastructure protections that ensure Secure Now, Undecryptable Later (SNUL) results.

Building a roadmap to quantum agility and security

Today, the scope and potential of post-quantum cryptography (PQC) solutions has expanded. Organizations and international standards bodies are identifying effective algorithms and developing cryptographic systems that can defend against both quantum and classical attacks.

Indeed, for a number of technical reasons, software based PQC is attracting increased attention. It's ex-

[1] The CIO's Guide to Quantum Computing
https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing

pected to take up a much larger market share in the future, because QKD (Quantum Key Distribution) requires substantial financial investments and IT resources. By contrast, software based PQC provides more security at a lower cost with reduced manpower and time.

For business leaders, following a security roadmap includes several key steps to build robust crypto-agility. From the outset, it's important to design a quantum-safe infrastructure along with applications and PQC solutions. The first step is to assess the level of organization-wide quantum risk and ensure that system-wide changes don't alienate end users or adversely effect functionality.

Preparing a secured system for quantum computing also requires devoting IT resources and significant financial investments. Since a full-scale transition to quantum security is expensive, decision-makers can choose one of three solution paths most appropriate to their organization's needs.

Choosing the right PQC solution path

Full-scale adoption of a PQC environment across a company's infrastructure represents the first option for deployment. However, organizational leaders need to consider the safety risks associated with new technology adoptions and the costs associated with full-scale conversions. A PQC approach also entails a difficult learning curve for IT teams as well as creating time and resource obstacles.

The second deployment option is for IT administrators to change their standard system ciphers to PQC quality. It offers a way to retain legacy technology and hardware while moving forward with quantum innovations that can meet evolving standards.

However, this approach can lead to unexpected issues related to compatibility standards between legacy systems and ciphers, resulting in additional costs. Moreover, each revision will generate resource and infrastructure effects that are the same as adopting a full-fledged PQC environment.

The third approach entails modifying the PQC algorithm, such as increasing key length or adding further security measures to the current system. However, this approach is not a fundamental solution and introduces problems that can require more resources, such as increased processor speed and additional memory.

Gaining cryptographic agility and quantum tolerance

For companies developing solutions with PQC technology, it's recommended to use existing systems and new solutions in parallel with the expertise provided by a professional consulting firm. In turn, organizations gain economic benefits by minimizing trial and error, reducing adoption costs and increasing efficiencies.

As part of the effort to bring quantum technology to the mainstream, IoT security provider Norma offers the Q Care series as an algorithm-agnostic solution that provides size optimization and side-channel immunity implementation of all NIST-configured PQC algorithms, from hardware and software.

Norma's goal is not only to protect sensitive data and critical infrastructure, but also to help implement secure IoT infrastructure with quantum security technology. The company's Q Care series is designed to enable companies to upgrade their hardware deployments (sensors, hardware security modules, etc.) to software (PKI, TLS, VPN, etc.) and achieve cryptographic agility and quantum tolerance as well as comply with current encryption standards.

31.Post-Quantum Cryptographic IP From Xiphera

by Steve Bush
https://www.electronicsweekly.com/news/design/eda-and-ip/post-quantum-cryptographic-ip-from-xiphera-2022-12/

Xiphera has announced intellectual property cores for implementing hardware post-quantum cryptography security on FPGAs and asics.

Such security is executed on classical computing platforms to protect against quantum computing based attacks.

Branded ‘xQlave’, the IP blocks are aimed at quantum-secure key exchange and digital signatures.

“Powerful enough quantum computers will be able to break current public-key asymmetric cryptosystems based on integer factorisation and discrete logarithms, compromising the entire basis of information and network security,” said Xiphera. “The xQlave family introduces IP cores for the post-quantum cryptographic algorithms recently announced as the winners of the competition by the American National Institute of Standards and Technology [NIST].”

The first product in the product family is for the Crystals-Kyber key encapsulation algorithm, and will be available for customer evaluation in January 2023.

This will be followed by further cores for that algorithm, balancing resources and performance, as well as for the Crystals-Dilithium digital signature algorithm.

“The xQlave family forms the core of Xiphera’s product offering for public-key cryptography in the future, and used together with traditional elliptic curve cryptography in hybrid encryption schemes, offers protection against quantum-computing attacks already today,” said company CTO and co-founder Kimmo Järvinen.

According to Xiphera, concerns have been raised about sensitive data being stolen today and stored for decryption when sufficient quantum computing power is available. It said that the American NSA and French ANSSI security organisations already recommend that systems designed and deployed today are quantum-secure-cryptography-ready.

Xiphera is based in Espoo Finnland, and develops cryptographic intellectual property for FPGAs and asics.