Crypto News

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

May 01, 2023

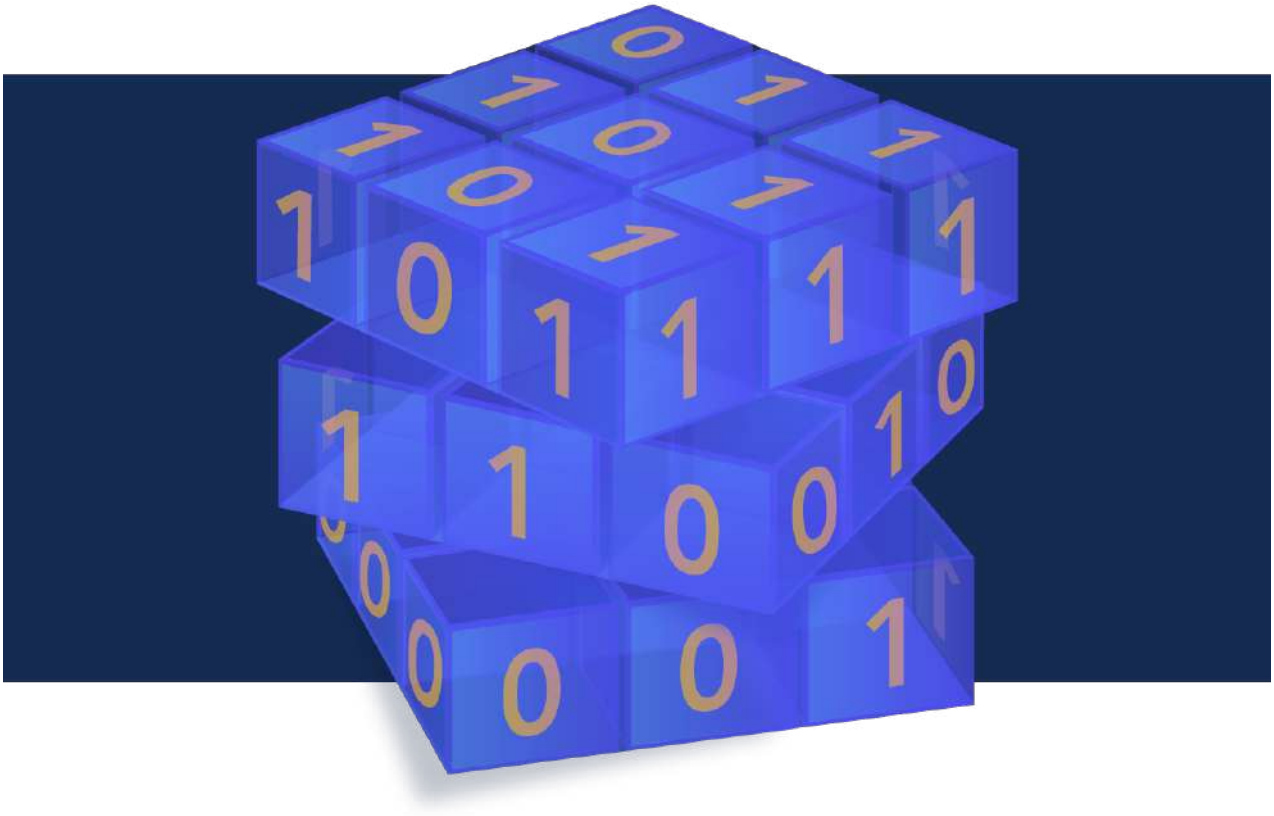


TABLE OF CONTENTS

Editorial

It's getting warmer outside and the news around Quantum Computing is getting hot. For those of us who work directly or indirectly with the healthcare industry in the United States, you'll want to read articles 1 and 30. Article 1 points out the importance of protecting patient data in a post-quantum world. This ranges from understanding how traditional cryptography will be impacted, threats to patient health, and even geopolitical risks from nation states amongst other risks. Scroll down to learn about all of the risks and solutions that you can implement which will help mitigate the risks of Quantum Computers. Then head over to article 30 to read about the federal mandates passed several months ago related to post-quantum encryption (one of the solutions outlined in article 1) that will eventually affect healthcare along with a number of other industries. These mandates were signed into law by the Biden administration for federal agencies but forward-thinking leaders will see its wider implications for their organizations. Don't fall behind when planning for a post-quantum world, because if you do, it'll already be far too late.

Another country that isn't taking Quantum lightly is India. They've really been upping the ante when it comes to Quantum technology. In articles 2 and 13, you can learn about their "National Quantum Mission" which was launched by the Department of Science and Technology of the Government of India. They are providing funding valued at $730 million from 2023 – 2031 for the mission which "aims to foster scientific and industrial research and development in Quantum Technology (QT) to accelerate economic growth, establish India as a global leader in Quantum Technologies & Applications (QTA), support national priorities such as digital India, Make in India, Skill India, and Sustainable Development Goals (SDG)." This government funding is in addition to other initiatives related to India's pledge to be Quantum ready so the total funding is significantly higher. In addition to the United States and India, other countries are also taking Quantum seriously. Take a look at articles 17, 20, and 22, to learn about what China, Germany, and France have done and plan to do in the future as it relates to Quantum Computing.

We are living in exciting times! Take a look and let me know what else you find interesting in this issue of Crypto News. Happy reading!

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

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

1.Protecting Patient Data: Why Quantum Security is a Must in Health Care

by Dave Krauthamer
https://securityboulevard.com/2023/04/protecting-patient-data-why-quantum-security-is-a-must-in-health-care/

When you visit the doctor or have a hospital stay, you and your patient data become elements in a vast, highly complex digital technology ecosystem. This is because you (as the patient) generate enormous volumes of data which is stored and analyzed across interconnected systems. The goal of all of this is improved health care outcomes, but the current health care digital landscape also represents a critical cyberattack surface. This is particularly true of medical devices and the internet-of-medical-things (IoMT). Security is a serious matter in health care, and most organizations involved in health care technology are busy implementing countermeasures against prevailing cyberthreats. More work is needed, especially considering the looming quantum computing threat to data encryption. This article examines the quantum threat to health care data and technology and offers some ideas on how this serious risk can be mitigated.

Understanding Health Care as a Technology Ecosystem

Healthcare is a field that runs on digital technology. Healthcare organizations deploy millions of connected medical devices that store personal patient data and real-time biometric data. These devices allow doctors and patients to communicate faster, more efficiently and, in some cases, more inexpensively than is possible with past communication methods. For instance, a direct digital heartbeat transmission is far faster and cheaper than a fax machine. In addition, back-end systems handle medical records storage, billing and operations.

A Brief Overview of the Quantum Threat to the Health Care Industry

Every medical device, computer server, network and storage array is vulnerable to cyberattack. Today, this means anything from ransomware to zero-day attacks–any threat vector that enables a malicious actor to interfere with health care processes or steal data. In the near future, this digital healthcare landscape will also be vulnerable to attacks from quantum computers.

Briefly, a quantum computer is a new generation of computing technology that utilizes sub-atomic particles and the principles of quantum mechanics to deliver exponentially faster computation capabilities than existing computers. There are many exciting potential uses for quantum computing, including in health care, such as protein folding. However, the technology is also expected to break today's "unbreakable" cryptographic keys that secure data and critical systems.

Security experts are worried, with good reason, that within a few years, today's current forms of cryptography will be rendered useless by the quantum threat. At that point, virtually all data and systems will be exposed to threats, including those systems that manage health care information. This would be catastrophic on multiple levels. The quantum crisis threatens patient health, the large and lucrative health care industry, society and even the United States' national security.

Threats to Patient Health

If all cryptography protecting the security and privacy of medical technology becomes inoperable, then patient health is at risk. Attackers could disrupt hospital networks and delay patient care. They could cause pacemakers, defibrillators, insulin pumps and other critical health devices to stop working. This could cause people to get sick or even die. Indeed, this type of thing has already happened. For example, in 2019 a ransomware attack on a hospital resulted in the death of a newborn.

Threats to a Vast, Critical and Lucrative Business

Health care is a multi-trillion-dollar industry. The quantum threat puts this enormous slice of the economy at risk. Even just one sector, the IoMT market, is rapidly accelerating, expected to go from a $14 billion valuation in 2017 to $158 billion this year.

Medical information is also valuable. Research suggests that it can be valued up to 50 times more than a stolen credit card on the black market. This is an attractive target for hackers.

Regarding legal liability and ethics, unsecured devices or device exploit comprise a violation of trust to patients. Device manufacturers have a fiduciary responsibility to protect patient data. Adding in regulatory penalties, such as HIPAA violations, the quantum threat's potential costs appear to be astronomical.

Societal Risks

Risks to individual patients are bad enough, but overall health care cyber risk exposure threatens the broader society. If health care systems, especially emergency services, are unavailable during a crisis, the public could be in danger. This is not as far-fetched a scenario as people might imagine. After all, ransomware attackers have targeted municipal government and law enforcement in tandem with hospitals. A quantum attack that devastates all such systems could destabilize the public order.

Geopolitical Risks

Health care information also figures into geopolitics and the world of intelligence. This may seem a bit cloak-and-dagger, but the reality is that adversarial nation-state intelligence services are stealing hundreds of millions of American health records. The 2015 Anthem breach is cited as an example. It's unclear exactly why they are doing this, but possible explanations include a desire to create a "social map" of the United States to identify spies. There is also a theory that the Chinese artificial intelligence (AI) industry is hacking American medical data to develop training data sets for medical AI software, which is considered a strategically important industry. The fascinating Wall Street Journal article "What Does Beijing Want With Your Medical Records?" explores this issue.

Regulatory Landscape

The government is taking a strong interest in cybersecurity for health care. U.S. federal agencies are expected to start mandating cybersecurity requirements through legislation such as the 2022 Protecting and Transforming Cyber Healthcare ("PATCH") Act, which requires a software bill of materials (SBOM), as mandated by president Biden's May 2022 executive order. These measures also expect medical devices to have greater cryptographic agility.

The pending Healthcare Cybersecurity Act of 2022 is a further call-to-action from the government. The bill wants to make cybersecurity a primary goal of health care organizations and equipment manufacturers. This includes the critical step of protecting legacy devices incapable of withstanding today's cyberattacks. The bill is poised to impose financial constraints, with Medicare payment policies incorporating

cyber expenses.

Quantum defense still needs to be added to the legislative agenda for health care, but it will almost certainly be included soon. The government is starting to mandate mitigations of the quantum threat in government systems. For example, the Cybersecurity and Infrastructure Security Agency (CISA) published guidance called “Preparing for Post-Quantum Cryptography” in 2022 in collaboration with NIST. Health care will likely follow.

Quantum Security Solutions for Health Care

It is important to start defending against the quantum threat now. Or, at a minimum, health care organizations can start preparing by assessing their cybersecurity to look for areas that will be vulnerable to a quantum attack. If health care companies want to follow the CISA/NIST guidance, they should start by inventorying their critical data and systems, including device operating systems. They ought to create an inventory of their cryptographic technologies and internal standards. This includes public key cryptography, which is most vulnerable to quantum attacks.

Health care organizations then need to move toward what is known as post-quantum cryptography, a new approach to cryptography that changes the way keys are generated, managed and used. Using advanced mathematical techniques, post-quantum cryptography methods can protect health care data from even quantum decryption processes.

2.What Will India’s New National Quantum Mission Achieve?

by Umakant Damodar Rapol
https://www.thehindu.com/sci-tech/science/national-quantum-mission-india-science/article66788784.ece

Sensors – systems that help detect electric and magnetic fields, rotation and acceleration, measure time, and image biological systems with increasing accuracy – are an inalienable part of essential enterprises like healthcare, security, and environmental monitoring today and practically indispensable for day-to-day life.

The National Quantum Mission, launched by the Department of Science and Technology of the Government of India, aims to catapult efforts across the nation to engineer and utilise the delicate quantum features of photons and subatomic particles to build advanced sensors that boost the value added by these enterprises and to support sustainable development.

The Union Cabinet approved the Mission last week at a cost of Rs 6,000 crore. It will be implemented from 2023 to 2031.

How can quantum physics help?

Classical sensors are based on familiar principles and as such their mechanisms are intuitive to us. In medical diagnostics, these sensors play a central role in sensing the very feeble signals emitted by atomic nuclei in tissues and detecting diseases. They sense the weak magnetic fields generated by neurons and map the brain’s activity, helping experts detect neurological illnesses at an early stage.

They are also used in the Global Positioning System (GPS) to measure small deviations in space and time, allowing us to build sophisticated transportation and logistics systems on the ground.

When we push the limits of these classical sensors by taking advantage of processes happening on the subatomic scale, our devices access a level of sensitivity that lets us develop game-changing applications.

Consider the 'squeezed states' of light. They overcome a detection limit that comes up when we use light to detect physical phenomena. This is because of Heisenberg's uncertainty principle: we can't measure the intensity and the phase of photons (the basic particles of light) with the same accuracy at the same time. That is, there is a natural limit on how accurately we can measure the intensity of light when it is reflected from or absorbed by objects or when the phase of light changes.

Quantum mechanics can help us overcome this barrier by allowing us to measure only the parameters of interest with higher accuracy ('squeezed states'), at the expense of parameters that are not of interest. How can technologies take advantage?

It is worth noting that quantum mechanics works counterintuitively to our experiences in the macroscopic world. This is because systems operating at atomic and subatomic scales are governed by phenomena like quantum superposition (like two circular waves adding up in the water when two pebbles are thrown), quantum entanglement (a characteristic that leads to knowing the properties of two distant particles instantaneously), wave-particle duality (particles behaving as waves and vice versa), and quantum tunnelling (particles sometimes finding their way through a barrier).

When these possibilities – which don't exist in the macroscopic world – are used in technologies, the technologies seem capable of doing wondrous things.

For example, an electron microscope takes advantage of wave-particle duality. An optical microscope uses visible light as the medium of imaging. An electron microscope uses electrons instead of visible light. The wavelength of electrons (considered as waves) can be reduced to a limit where an electron microscope can image nanometre-sized objects – a task impossible with visible light.

The results of quantum mechanics are not limited to sensors. The successive application of the principles of quantum mechanics has led scientists to discover semiconducting devices like transistors and superconductors and to understand the forces between atoms in molecules. It gave rise to the boom in semiconductor technology, clean energy, and the development of novel drugs.

In the 21st century, scientists worldwide have been able to control and harness quantum mechanical features to build devices that are coming to define new paradigms in several sectors, leading to the second quantum revolution, or Quantum 2.0. This is expected to address humankind's need for faster transportation, faster and more secure communication, short lead-times in designing drugs, securing national borders, and exploring deep space.

How will Quantum 2.0 help India?

On the Quantum 2.0 front, India has thus far had small-scale and isolated efforts led by various scientists in academia, government laboratories, and some other facilities. These scattered efforts have led to restricted capacity in the field and with a limited translatability into useful products.

The National Quantum Mission is designed to boost these efforts through coordinated efforts to consolidate existing knowhow and create a nationwide knowledge generation, translation, and indigenisation endeavour.

As far as quantum-sensing is concerned, the Mission will focus on research and technology development to build a plethora of devices and systems, including

Magnetic sensors that can sense magnetic fields that are a million-times weaker than the earth's magnetic field, using virtual atoms trapped in diamonds, atoms cooled and trapped at near absolute-zero temperature, collections of atoms at room temperature, etc.

Precise clocks that will lose less than one second in more than 300 billion years, allowing us to develop navigation devices that are more than 1,000-times precise to help study the origin of the universe – an open question in astrophysics

Navigation devices that can operate autonomously, without the need for GPS signals – an important part of autonomous driving systems and deep space navigation

Affordable sensors that can detect anatomical changes within human bodies with minimal intervention

The Mission will also help attain these at a cost that is affordable and scalable for a wide range of applications.

3.Quantum Advantage Coming by 2027: Omdia

by Berenice Baker
https://www.quantumbusinessnews.com/infrastructure/quantum-advantage-coming-by-2027-omdia

Examples of "quantum commercial advantage" — an improvement in speed, cost, efficiency or quality over the typical classical computing commercial alternative for a problem of commercial interest — will become common by 2027, according to a new study.

The report from Omdia also states that there is a high probability that the quantum computer industry will successfully produce fault-tolerant scaled quantum computers of more than 1,000 logical qubits with robust quantum error correction.

Quantum Computing Forecast 2023 suggests that these examples will draw significant new interest, investment, and activity to the quantum market, meaning the likelihood of a "quantum winter" – when investors and technology companies shy away from investment – is minimal.

By 2027, Omdia anticipates that examples of "quantum commercial advantage" — an improvement in speed, cost, efficiency or quality over the typical classical computing commercial alternative for a problem of commercial interest—will become common.These examples will draw significant new interest, investment and activity to the quantum computing market.

Nevertheless, Omdia says that fault-tolerant scaled quantum computers will not arrive before 2030 at the earliest, and they could take 10 to 15 years to achieve.

"If fault-tolerant scaled quantum computers are possible, we also expect that new quantum algorithms for combinatorial optimization and new approaches for quantum machine learning will be found to enable exponential speedups in these areas alongside exponential speedups for the physical simulation of quantum mechanical systems," said report author and Omdia chief quantum computing analyst Sam

Lucero.

Recommendations for Adopters

The report also contains several recommendations for enterprises considering adopting quantum computing.

- **Get started now:** Quantum computing's shift from a niche technology to a mainstream sensation could be just as sudden as the recent activity with generative artificial intelligence and large language models. Organizations should start now with learning and experimenting with quantum computing to be ready when the shift happens.
- **Co-develop hardware:** Enterprises with sufficient resources should consider working with a quantum computer hardware vendor to co-develop a solution that is configured to precisely match their quantum algorithm and application needs. This may be a near-term way to push ahead of competitors that are experimenting with general-purpose quantum computers.
- **Create an algorithm:** There is still a shortage of quantum algorithms and quantum machine learning approaches that enable an exponential speedup. Enterprises should consider investing in developing such an algorithm for their application as a way of developing defensible intellectual property rights.
- **Access government funding:** Many governments regard quantum technology as a national and economic security priority. Significant funding and other aid may be available to businesses adopting it.
- **Leverage hyperscalers:** Many large cloud service providers are helping the ecosystem by supplying access to multiple third-party quantum computing hardware, which enables easier experimentation by adopters.

4.Joint Statement of the United States of America and Republic of Korea on Cooperation in Quantum Information Science and Technologies

https://www.state.gov/joint-statement-of-the-united-states-of-america-and-republic-of-korea-on-cooperation-in-quantum-information-science-and-technologies/

The United States of America and the Republic of Korea, building upon their shared values and strong alliance, intend to pursue cooperation in quantum information science and technology (QIST) for the peace and prosperity of the citizens of both countries.

We understand that science and technology are key drivers of innovation in society and the economy, and that collaborative and transnational efforts in research and development are important to accelerating innovation.

We recognize that QIST is a critical and emerging technology, which enables the development of powerful computers, more secure communications networks, and more precise and accurate sensors, by exploring new ways to acquire, transmit, and process information using quantum mechanics.

We assert that the emergence of such technologies provides opportunities to enable wider scientific endeavors and to develop new applications for using QIST to explore grand societal challenges, potentially including global health, climate change, and efficient resource use.

We affirm that a skilled workforce and an increased awareness of applications are essential for the progress of QIST and the development of quantum-enabled economies, and that diverse efforts are required to encourage broad and inclusive participation in QIST, including public awareness campaigns, educational initiatives, apprenticeships, quantum and interdisciplinary skill building, and reskilling programs.

We acknowledge that the QIST ecosystem, consisting of stakeholders from various areas, including academia, government, and the private sector, is global and interconnected. The exchange and integration of ideas, expertise, and creativity is critical for expanding basic understanding and accelerating the deployment of QIST.

Building on the Agreement Relating to Scientific and Technical Cooperation between the Government of the United States of America and the Government of the Republic of Korea signed at Washington on July 2, 1999, as extended (the “S&T Agreement”), we intend to advance our shared vision of QIST as follows:

We intend to embark on good-faith cooperation underpinned by our shared values including freedom of inquiry, fair competition, openness and transparency, accountability and reciprocity, protection and enforcement of intellectual property, rigor and integrity in research, research security, and democratic values.

We commit to create inclusive scientific research communities and tackle cross-cutting issues of common interest such as equity, diversity, inclusion, and accessibility, so that every person may fully participate and have an equal opportunity to succeed.

We strive to facilitate interactions between government, academia, and the private sector to understand research trajectories in QIST. In turn, these interactions can lead to the identification of overlapping interests and opportunities for future scientific cooperation to accelerate the societal benefits of this nascent field and remain responsive to its as-yet-unknown implications.

We intend to enable opportunities to build a trusted global market and supply chain for QIST research and development (R&D), and support economic growth, by engaging the private sector and industry consortia.

We plan to leverage regular bilateral and multilateral opportunities to discuss QIST matters, including standardization, and technology protection considerations, where international collaboration is key.

We intend to promote joint research in QIST, including personnel exchanges and the sharing of QIST-related methodologies and data on voluntary and mutually agreed terms, to develop the next generation of scientists and engineers vital to expand the field. Cooperation pursuant to this Joint Statement is subject to the terms of the S&T Agreement.

The United States of America and the Republic of Korea look forward to deepened bonds of friendship and understanding between our two countries, and to mutual contributions for the enhancement of QIST, based on increased cooperation in the field.

5.Public Comment Sought on Post-Quantum Cryptography Migration

by Kimberly Underwood
https://www.afcea.org/signal-media/cyber-edge/public-comment-sought-post-quantum-cryptography-migration

Seeking comments from industry, government and academia, the National Cybersecurity Center of Excellence (NCCoE) issued a preliminary guide on practices related to migrating away from legacy cryptography. The draft document, NIST Special Publication (SP) 1800-38A, Migration to Post-Quantum Cryptography, is open for comment through June 8.

The NCCoE is housed at the National Institute of Standards and Technology (NIST), which is preparing and standardizing quantum-resistant public-key cryptographic algorithms. The NCCoE plans to update the preliminary draft based on the input received and will publish additional volumes for comment to guide the widespread adoption of "safe" cryptography.

"Advances in quantum computing could compromise many of the current cryptographic algorithms being widely used to protect digital information, necessitating replacement of existing algorithms with quantum-resistant ones," the NCCoE indicated. "Previous initiatives to update or replace installed cryptographic technologies have taken many years, so it is critical to begin planning for the replacement of hardware, software, and services that use affected algorithms now so that data and systems can be protected from future quantum computer-based attacks."

In particular, the organization is seeking feedback on the workstreams needed to move to quantum-resistant solutions—such as identifying gaps that exist between post-quantum algorithms and their integration into protocol implementations—so they can help accelerate the adoption and deployment of post-quantum cryptography (PQC).

The agency warned that legacy cryptography in use today—like the Rivest-Shamir-Adleman algorithm (widely known as RSA encryption), Elliptic Curve Diffie-Hellman and the Elliptic Curve Digital Signature Algorithm—need to be updated, replaced or significantly altered for application of new quantum-resistant algorithms.

"The new algorithms will likely not be drop-in replacements for the quantum-vulnerable algorithms," the NCCoE warned. "They may not have the same performance or reliability characteristics due to differences in key size, signature size, error handling, number of execution steps required to perform the algorithm, key establishment process complexity, etc."

Moreover, entities may not be aware of the breadth and scope of the dependencies on legacy cryptography across all of their products, services and operational environments. Given this possible lack of visibility, the NCCoE recommended building a complete inventory of where organizations are using cryptography, including across software vendors or services, and having an understanding of where the vulnerable legacy cryptography is housed, on-premise or over the internet, for example. In addition, organizations need to know what data is associated with the keys and any interdependencies.

"Increased use of discovery tools will have the added benefit of detecting and reporting the use of cryptographic algorithms that are known vulnerable to non-quantum attacks," the NCCoE stated. "Maintain-

ing connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms will require careful planning. Furthermore, an organization may not have complete control over its cryptographic mechanisms and processes so that they can make accurate alterations to them without involving intense manual effort."

William Newhouse and Murugiah Souppaya from NIST, William Barker from Dakota Consulting and Chris Brown from The MITRE Corporation prepared the draft. Comments will be accepted for this particular draft through just before midnight on June 8, 2023. Click here and submit comments via a web form on the project page. Questions can be sent to applied-crypto-pqc@nist.gov.

"Our strategy for future phases will build iteratively to produce recommended practices for algorithm replacement, where in some cases interim hybrid implementations are necessary to maintain interoperability during migration," the NCCoE said. "We invite feedback from the larger PQC community of interest to identify future workstreams that will accelerate the adoption and deployment of PQC."

6.RSA Cryptographers' Panel Talks Quantum Computing and AI

by Mathew J. Schwartz
https://www.govinfosecurity.com/rsa-cryptographers-panel-talks-quantum-computing-ai-a-21852

Prepare now for the coming of quantum computing and its potential ability to crack current cryptographic systems, warned panelists of the annual Cryptographers' Panel at RSA Conference. Despite their status today as expensive science projects, superfast computers that use atom-level states of uncertainty are likely a matter of time, leading to worries that today's encryption standards are destined for obsolescence.

While hype is high around quantum computing, panelist Radia Perlman, a fellow at Dell EMC who's an expert in network routing protocols and network security, said there's a clear imperative for "the good guys" to research the risk posed by quantum computers because "the bad guys" will be doing the same. If that happens, she said, "we're all going to have to replace our current public key algorithms."

At least some organizations should organize for the potential eventuality that quantum computers will break current cryptographic systems. Longtime panelist Adi Shamir - the S in the RSA cryptosystem and a professor of computer science Israel's Weizmann Institute - said the big danger is that a quantum computer able to crack today's encryption could well be developed in 30 years, and "the NSA or other bad guys are going to record everything that everyone says today, then wait until quantum computers become available and then break the cryptography."

For anyone who needs to keep a set of data secure for more than 30 years, his advice is simple: Don't rely on public key cryptography.

Shamir added that "99.99% - and maybe a few additional nines - of what's being encrypted today and signed does not require a 50-year secure life," given that most emails are about banal matters - think plans for lunch. Even sensitive information, such as an organization's product development efforts, might become public knowledge in 12 months.

Whether quantum computers will ever be able to crack today's cryptosystems remains unclear. Public key algorithms will be affected, said panelist Anne Dames, a distinguished engineer and head of Crypto-

graphic Technology Development at IBM. As a defense for symmetric key and hashing, cryptographers may be able to increase the key or message digest sizes, she said.

The U.S. National Institute of Standards and Technology last year picked four algorithms designed to resist decryption attacks mounted by a quantum computer, as part of its effort to set a post-quantum cryptographic standard. Panelists said NIST has signaled that it might expand the shortlist, in part because all four use a similar mathematical approach, which isn't ideal.

Chatbots: Security Peril and Promise

Among the hot topics at RSA Conference 2023, arguably the hottest is the impact of AI and machine learning, driven by chatbots such as ChatGPT. "What they seem to be pretty good at is human engineering," said Whitfield Diffie, who with Martin Hellman pioneered public key cryptography in the early 1970s said.

Shamir said until last year, he thought AI might have some use cases purely on the defensive side of cybersecurity and very few offensive use cases.

"I've completely changed my mind as a result of last year's developments, including ChatGPT, etc.," he said. "I now believe that the ability of ChatGPT to produce perfect English, to interact with people, is going to be misused on a massive scale" and to "have a major impact on social engineering."

Blockchain's Bad Year

If ChatGPT is ascending the hype scale, blockchain's star seems to be falling.

"Blockchain has been having a bad year," Diffie said, perhaps due only in part to revelations such as how collapsed cryptocurrency exchange FTX was being run (see: *3rd FTX Official Pleads Guilty to Criminal Charges*).

"Well, there's cryptocurrencies and there's blockchain," Perlman said.

She said her long-standing advice to project teams interested in applying blockchain remains the same: Evaluate different strategies for accomplishing your goal, "and if that is blockchain, which is unlikely," then select that, she said, to laughter from the audience.

An engineer once told her their manager was demanding blockchain be used. Her advice was: "Look at all the alternatives, choose the best one, build that, then tell your manager you built it with blockchain; they'll never know the difference."

7.Quantum Cybersecurity Threat Takes Center Stage at CyberUK

by Berenice Baker
https://www.iotworldtoday.com/security/quantum-cybersecurity-threat-takes-center-stage-at-cyberuk

The cybersecurity threat that quantum computers pose to national infrastructure was a key focus of CyberUK, the U.K. government's flagship cyber event held this week.

Delivering the keynote opening address in Belfast, Northern Ireland, newly appointed National Cyber Security Center (NCSC) CEO Lindy Cameron said that when it comes to quantum technologies, organizations must factor the impact of quantum computing into their long-term roadmaps.

“We must all prepare for the rollout of post-quantum cryptography over the coming years, safeguarding the security of the cryptography that underpins the internet, and therefore the digital economy,” she said.

“Major global vendors will, in due course, update their operating systems and cryptographic libraries with internationally accepted and standardized quantum-resistant solutions.”

Cameron added that organizations and individuals with standard office set-ups will benefit from those improvements automatically if they update their cybersecurity solutions regularly. However, some sectors have more specialized needs, either because they have bespoke infrastructure or where there are practical constraints on regular updating.

Cameron said the NCSC can offer support in these circumstances before going on to highlight some potential benefits of quantum computing.

“As well as these challenges, the U.K. can also harness the nearer-term opportunities that quantum computing will provide, such as the chance to solve complex logistics and simulation problems in a sustainable and energy-efficient way, a real boost to our digital economy,” she said.

Commenting on the event, senior vice-president of post-quantum cryptography company PQShield Ben Packman said:

“We welcome the government’s renewed focus on improving the cybersecurity of the U.K.’s critical national infrastructure, which is under increased pressure from foreign adversaries. Post-quantum cryptography is an essential part of this.

“The U.S. is currently the global superpower when it comes to quantum-secure technology and legislation, but the U.K. is not far behind, with impressive local capabilities and talent. The government can leverage this to lead this emerging sector on a global scale.

“Cryptography modernization is key, and to achieve this on a suitable timescale, the government must continue to support industry with a clear strategy and guidance, boosted by sufficient investment.”

8.How Government Action Is Providing a Blueprint for Post-Quantum Preparedness

by Samantha Mabey
https://www.entrust.com/blog/2023/04/how-government-action-is-providing-a-blueprint-for-post-quantum-preparedness/

The quantum threat is out there. And it’s not a matter of “if”, but a matter of “when”. While the specific

"when" is unknown, it's generally accepted that in anywhere from 7-10 years a quantum computer will be capable of breaking the traditional public key cryptography in use today.

While that might seem pretty far out, we do know that the steps to get ready and then ultimately migrate to post quantum (PQ) cryptography will take several years. We're not talking about a crypto refresh cycle here. We're talking about something an order of magnitude more involved and challenging than anything that's been done before. That's why we are of the position that the time to prepare for post quantum is now. And we are not alone in that thinking.

If you've been keeping up with the news, I'm sure you've noticed the uptick in government action that's been taking place around PQ lately. And this has been happening at a global level. What's nice about some of these directives is that they are providing (or in our case validating) the blueprint for what needs to be done in order to prepare for post quantum.

This past September the NSA released the CNSA 2.0 Timeline which advised that algorithms for software and firmware signing, should begin transitioning immediately. The algorithms they recommend implementing are based on the NIST round 3 finalist algorithms, which were announced last summer. They're not trying to get ahead of the process by publishing these requirements ahead of the final selections for standardization, but rather hoping that it will generate awareness of what needs to be done and allow time to "plan and budget for the expected transition".

Last spring and prior to the NSA announcement, the White House had issued the "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems". It then followed up with another memo in November 2022 which provided additional direction and some clear actions to federal agencies in preparing for the migration to PQC. The first two steps were:

- **Designate a lead**. The memo stated that within 30 days (which brought us to December 28, 2022), agencies needed to designate a lead for collecting cryptographic information systems. This should be the first step for any organization in order to ensure there is central ownership and oversight over the strategy and transition.

- **Perform a cryptographic inventory**. The memo then clearly requires agencies to inventory cryptographic hardware and software systems by May 4, 2023. Whether ensuring you have the right technology in place to support the requirements of PQC, or ensuring visibility into all your cryptographic assets (keys, certificates, etc.), this will likely be one of the more challenging and time consuming tasks. It will also help determine if you're crypto agile which will be key when it comes to implementing PQC.

While final implementation direction and migration strategies are still to come, the memo also suggests that agencies should be working with their vendors to identify post quantum cryptography testing opportunities within their networks. This will be critical universally as standards (when they come) are one thing, but approved working deployments are another. And the "Quantum Computing Cybersecurity Preparedness Act" indicates that agencies will need to quickly migrate to quantum resistant systems once those standards are identified.

So, all eyes will remain on the NIST PQC Competition to see what the final recommendations for standardization are, but in the meantime, there is much to do. And it really is time to get going.

9.The Agency Continues its Post-Quantum Cryptography Push as it Looks to Create Guidance for All Sectors.

by Alexandra Kelley
https://www.nextgov.com/technology-news/2023/04/nist-releases-draft-post-quantum-encryption-document/385580/

The latest step in post-quantum cryptography guidance is helping organizations identify where current public-key algorithms will need to be replaced, as the National Institute of Standards and Technology continues its push to fortify U.S. digital networks ahead of the maturity of quantum computing.

A new draft document previews—and solicits public commentary on—NIST's current post-quantum cryptography guidance.

Current goals outlined in the working draft include helping entities locate where and how public key algorithms are utilized in encryption schemes, developing a strategy to migrate these algorithms to quantum-resilient substitutes and performing interoperability and performance testing.

"Organizations are often unaware of the breadth and scope of application and functional dependencies on public-key cryptography within their products, services and operational environments," the draft document reads.

In conjunction with the National Cybersecurity Center of Excellence, NIST is seeking public feedback on the draft guidance, hoping to draw from industry's expertise to form ubiquitous best practices in quantum-resilient cryptography.

A major theme of the document is to help organizations understand the security architecture in their networks so that they firmly grasp where post-quantum security measures will need to be implemented and where to prioritize modernization. NIST also aims to compile a definitive inventory of software vendors to support post-quantum cryptography migration.

Bill Newhouse, a cybersecurity engineer with NIST and NCCOE, told *Nextgov* that the comments will ideally inform regulators which cryptographic algorithms are in use to protect digital networks to better understand how migration will occur.

"In advance of final post-quantum cryptography algorithm standards, discovery activities are a necessary first step to learn which cryptographic algorithms are being used today to protect data and communications," he said. "From this discovery step, migration prioritization decisions can begin to be made."

From this perspective, interoperability and performance considerations will be taken into account for several draft post-quantum cryptographic algorithms. Newhouse said that these algorithms will be implemented for key exchanges and digital signatures security protocols.

The new guidance follows NIST's ongoing effort to finalize its quantum-resistant algorithms in 2024 after identifying four in 2022.

The agency then announced partnerships with 12 private sector companies to help develop quantum-resilient algorithms and implement them nationwide, including Amazon Web Services and Microsoft.

Both of these efforts follow President Joe Biden's National Security Memorandum leveraging federal resources to help all U.S. digital systems migrate to quantum-resilient cybersecurity standards by 2035.

10.QuSecure's Leading Post-Quantum Cybersecurity Solution Wins Next-Gen Quantum Computing Global InfoSec Award During RSA Conference 2023

by Dan Spalding
https://www.businesswire.com/news/home/20230424005054/en/QuSecure%E2%80%99s-Leading-Post-Quantum-Cybersecurity-Solution-Wins-Next-Gen-Quantum-Computing-Global-InfoSec-Award-During-RSA-Conference-2023

QuSecure™, Inc., a leader in post-quantum cybersecurity (PQC), today announced that its industry-leading PQC solution QuProtect™ has won the coveted Global InfoSec Award from Cyber Defense Magazine (CDM), the industry's leading electronic information security magazine, as announced at the RSA Conference 2023. QuProtect was named the best solution in the Next-Gen Quantum Computing awards category.

This is Cyber Defense Magazine's tenth year of honoring InfoSec innovators from around the Globe. The judges were CISSP, FMDHS, and CEH certified security professionals who voted based on their independent review of the company submission and materials on the website. CDM has a flexible philosophy to find more innovative players with new and unique technologies, vs. only larger enterprises.

"It is extremely rewarding to be recognized at the RSA Conference by this esteemed panel of security judges as the leading solution in next-generation quantum computing," said Skip Sanzeri, QuSecure co-Founder and COO. "Our QuProtect solution enables organizations to protect their communications and secure private information as the world accelerates toward a quantum future, due to the looming threat of quantum computing's ability to break the public key encryption we currently use. QuProtect's post-quantum technologies are differentiated in the industry and uniquely provide secure, interoperable cybersecurity to protect networks from today's classical threats and future quantum threats."

QuSecure's QuProtect software enables organizations to leverage quantum-resilient technology to prevent today's cyberattacks, while future-proofing networks and preparing for quantum cyberthreats. It provides quantum-resilient cryptography, anytime, anywhere and on any device. QuProtect software uses an end-to-end quantum-security-as-a-service architecture that addresses the digital ecosystem's most vulnerable aspects, uniquely combining zero-trust, next-generation post-quantum-cryptography, crypto agility, quantum-strength keys, high availability, easy deployment, and active defense into a comprehensive and interoperable cybersecurity suite. The end-to-end approach is designed to protect the entire information lifecycle as data is communicated, used and stored.

"QuSecure embodies three major features we judges look for to become winners: Understanding tomor-

row's threats today, providing a cost-effective solution, and innovating in unexpected ways that can help mitigate cyber risk and get one step ahead of the next breach," said Gary S. Miliefsky, Publisher of Cyber Defense Magazine.

The QuProtect solution is the industry's most advanced quantum safe solution providing quantum-resilience for today's critical communications, including network, cloud, IoT, edge devices, and satellite communications. Using QuProtect, organizations can implement PQC across all devices on the network with minimal disruption to existing systems, protecting against current classical and future quantum attacks which could irreparably disrupt industries and infrastructures across government and commercial sectors; at the same time solving today's complex compliance challenges, such as bring-your-own-device (BYOD) and work-from-home policies.

11.QuSecure Collaborates with Red Hat to Deliver Enhanced Post-Quantum Cryptography Modernization

by Dan Spalding
https://www.businesswire.com/news/home/20230421005309/en/QuSecure-Collaborates-with-Red-Hat-to-Deliver-Enhanced-Post-Quantum-Cryptography-Modernization

QuSecure™, Inc., a leader in post-quantum cybersecurity announced today a collaboration with Red Hat aimed at providing enhanced classical and post-quantum cybersecurity solutions to customers in both the public and private sectors.

QuSecure's cutting-edge post-quantum cybersecurity technology, supported on Red Hat Enterprise Linux, Red Hat OpenShift and Red Hat Ansible Automation Platform, is designed to deliver a classical and post-quantum security solution that can protect against modern cyber threats. The QuSecure solution enables organizations to address crypto modernization efforts that government and private enterprises are undertaking to implement a zero-trust quantum resilient architecture before quantum computers begin decrypting today's data.

"The QuSecure offering is a testament to the power of collaboration and innovation," said Red Hat's Anna Levine, Senior Director, Public Sector Sales, Defense and National Security Programs. "This comprehensive security solution brings together the best of both worlds: QuSecure's advanced post-quantum cybersecurity technology supported on Red Hat open-source platforms. With this collaboration, we aim to empower organizations of all sizes with the tools they need to safeguard their digital assets against modern cyber threats."

QuSecure offers a range of features including advanced threat detection and prevention, enhanced data encryption and real-time monitoring and reporting. Additionally, the solution is designed to more seamlessly integrate with existing IT systems and infrastructure, minimizing disruptions and enabling improved efficiency.

"After years of discussion, the time has finally come for enterprise and government entities to take action and remediate their systems against the imminent quantum threat," said Dr. Garrison Buss, Chief Strategy Officer at QuSecure. "We applaud Red Hat for working so closely with us to empower these stakeholders to complete a low-risk upgrade to their currently vulnerable networks with the latest in modern

cryptography, breathing new life into their existing infrastructure and allowing them to implement security measures to help protect their systems for the next decade and beyond."

QuSecure's offering, supported on Red Hat open hybrid cloud and automation platforms, provides public and private organizations of all sizes with a powerful new solution for safeguarding their constituents and customers' digital assets. Further updates around this release will be announced by QuSecure at Red Hat Summit 2023 on May 23-25 in Boston.

12.The Race to Protect Networks Against Quantum Computing Powered Cyber Attacks

by Andrew Wooden
https://telecoms.com/521282/the-race-to-protect-networks-against-quantum-computing-powered-cyber-attacks/

Quantum computing, the next stage in supercomputing based on mind bending quantum mechanics principles, is getting more and more column inches as we appear to be getting closer to it reaching sufficient reliability and subsequent widespread availability.

The benefits are not precisely defined, but in a nutshell the vastly greater computing horse-power might be used to cure diseases, crack complicated economic problems, and basically could be used to solve any sort of complex problem the future might throw at us.

On the downside, it could also render current network cryptography and security basically irrelevant – a worrying prospect were it to get into the wrong hands.

What is Quantum Key Distribution?

LuxQuanta is a Barcelona based firm which deals in Quantum Key Distribution (QKD) systems, which are designed to be integrated into existing network infrastructure and bolt on a 'quantum-safe' layer of security on top of mathematical cryptographic techniques.

The pitch is that cryptographic techniques used today are not future-proof, because they will be easily hackable by quantum computers once they reach a specific capacity. What QKD, or Quantum Cryptography does is use quantum mechanical properties to create a shared key using an optical fibre or through free space, and using quantum signals (weak light pulses) it can detect hacking attempts. This, claims LuxQuanta makes the shared key resilient against an attack from a quantum computer. We spoke to Vanesa Diaz, Chief Executive Officer at LuxQuanta, to find out more.

"What we do is instead of relying on a mathematical problem to deliver this key that you will use to encrypt your information, is use the same link that we're going to use to transmit the data to transmit information so weak in the form of photons, that these photons enter into the quantum realm," says Diaz. "So it makes that channel, that optical fibre where I'm sending the information, super secure because if anybody tries to sneak in while I'm sending the information of the key, I will be able to tell.

"So at the end what you obtain from these two machines now connected at both sides of the link that

you want to protect, they deliver a key to encrypt our server, and then you start encrypting the information as you would have done previously. So that's the beauty of it, we deliver a technology that is unhackable and is future proof because we don't care whether you attack us with a quantum computer, or two or three – at the end we're relying on the laws of quantum physics and those are unbreakable."

"The [consultants] that we work with, they estimate the quantum key distribution market should reach $5 billion in revenue by 2031. That's a hockey stick in terms of market growth and I believe that we are definitely on the right pathway towards… it's getting intense."

When it comes to defending against quantum powered threats from hackers, as with most things there is more than one way to skin a cat – though LuxQuanta (unsurprisingly) pitches QKD as the gold standard.

"There is a discussion out there in the industry as to whether you should rely on software, meaning more complex mathematical problems – this is post quantum cryptography – and that definitely has an application for us. They are allies because it's easier always to offload software or get software from someone and install it in your network rather than investing in hardware. But it's true that if you really, really want to have the guarantee that nobody can hack it, absolutely nobody, then you do have to go to Quantum Key Distribution. And that's how things are."

The dangers of quantum computing powered hacks

So that's the QKD sub-sector in a nutshell, but where are these quantum powered attacks of the future going to come from? Diaz argues it will be the same players that already engage in malware and ransomware attacks, but this time armed with bigger guns.

"This is crime, organised crime. Here in Spain we've had a cyber attack to a hospital, it happened twice, and they are asking them for money to give back the information that they have stolen. It's just pure crime out there. The geopolitical context, protecting your own governmental information, is something that has been done for the beginning of time and that continues. So it's not that the enemy has changed really, the enemy for each potential use of this technology is pretty much the same. In the end, everybody is concerned about protecting the confidential data from any potential attacker."

Quantum chips in their present form live in facilities owned firms like IBM and are contained within in large expensive housings designed to keep them at temperatures colder than outer space, in order for the mind-bending physics to operate. A bad actor making use of quantum computing to provide a greater threat than can currently be mustered would in some way shape or form need access to this currently rare commodity, or future iterations of it. But Diaz thinks eventually, the technology will be made available to everyone, and that could just as easily include cyber-criminals.

"I believe that there will be models that will make quantum computing accessible to everybody. Same as today. It is being made available… you can log in, you can [run] algorithms there. So I think that the bad guys always find a way, that's for sure… the ones that have big resources, they could always source the hardware themselves. These manufacturers of quantum computers, eventually the target is to sell them. So I really believe someone can acquire them and then do whatever they want to with them."

Balancing the opportunities of quantum computing with the risks

When it comes to the tech firms developing quantum computing you do get the sense that they are cognisant of the potential dangers of it getting into the wrong hands, and are there appears to be a good amount of effort put into developing tools to mitigate the harms, in a way that you don't get the sense of with AI development.

"One of the messages that I've tried to convey or the in the industry is precisely that – you don't take

these things lightly," continues Diaz. "[Some] say quantum computers are still a long way down on the road – not really, if you look at the latest estimations you hear as close as 2030. Some people say that it is not irrational thinking that the worst case scenario is 2027. That's around the corner from now. So that's why I think people are waking up to that and that's the reason there is a lot of interest from all sorts of verticals.

"It is not only about telecommunication operators anymore, not at all. People from the food industry have come to us… because they always have a department in all these verticals that are looking at new technologies, and they look at potential hazards and how to protect themselves. There is always at least a team of people in each of these verticals looking into quantum technologies, all of them, and so there is a lot of traction from them now. Where do I need to protect my information? How can I use Quantum Key Distribution? I think they are grasping now the real risk. You don't have so many years to prepare yourself, so the sooner you start, the better."

13.India Announces $730 Million-Plus National Quantum Mission

by Matt Swayne
https://thequantuminsider.com/2023/04/20/india-announces-730-million-plus-national-quantum-mission/

The Union Cabinet approved the National Quantum Mission (NQM) with a total cost of Rs. 6003.65 crore — about $730,297,000 US — from 2023-24 to 2030-31, according to PM India and other press reports.

According to the site, the mission aims to foster scientific and industrial research and development in Quantum Technology (QT) to accelerate economic growth, establish India as a global leader in Quantum Technologies & Applications (QTA), and support national priorities such as digital India, Make in India, Skill India, and Sustainable Development Goals (SDG).

50-1000 Physical Qubits

The NQM has set ambitious targets to develop intermediate-scale quantum computers with 50-1000 physical qubits within 8 years using various platforms such as superconducting and photonic technology. It also aims to establish satellite-based secure quantum communications between ground stations within India and with other countries over a range of 2000 kilometers, as well as inter-city quantum key distribution over 2000 kilometers and multi-node Quantum network with quantum memories.

The program will also focus on developing high-sensitivity magnetometers in atomic systems and Atomic Clocks for precision timing, communications, and navigation. Additionally, it will support the design and synthesis of quantum materials such as superconductors, novel semiconductor structures, and topological materials for fabrication of quantum devices. Single photon sources/detectors and entangled photon sources will be developed for quantum communications, sensing, and metrological applications.

Thematic Hubs

To promote research and development in QT, four Thematic Hubs (T-Hubs) will be established in top academic and National R&D institutes, focusing on Quantum Computing, Quantum Communication, Quantum Sensing & Metrology, and Quantum Materials & Devices. These hubs will generate new knowledge through basic and applied research and contribute to the mission's objectives.

The NQM is expected to have a significant impact on various sectors including communication, health, finance, energy, drug design, and space applications. By fostering a vibrant and innovative ecosystem in QT, India aims to become a global competitor in quantum technology development. The mission aligns with national priorities and initiatives such as Make in India, Skill India, and Stand-up India, and will contribute to India's vision of becoming self-reliant and achieving sustainable development goals.

14.What Is The Purpose of Post-Quantum Cryptography?

by Tony Fyler
https://techhq.com/2023/04/what-is-the-purpose-of-post-quantum-cryptography/

What is the purpose of post-quantum cryptography? The basic, white bread answer would be "to keep all your secret stuff safe in the apparently imminent age of quantum computing, when standard cryptographic algorithms will be worth less than the paper on which you print them out."

That's it in a nutshell. Quantum computing, a development that's set to *massively* increase the processing power and speed of computers as we know them, is, according to plenty of cryptographic experts, likely to pull on the thread of all known, pre-quantum cybersecurity, and keep pulling until all our carefully constructed cryptography is just a pile of numbers around our naked, exposed ankles.

Post-quantum cryptography is a collective term for an ever-growing group of methods that will allow quantum computing to exist while still protecting all our secrets (like bank account numbers, Netflix passwords etc, but *also* like access codes to nuclear or chemical laboratories, government buildings, national critical infrastructure systems and more). Without the ability to have and keep secrets, the world as we've come to know it would stop functioning in a big, big hurry.

Public-key encryption.

The problem as it exists is that a lot of our pre-quantum cybersecurity is based on public-key technology. What's public-key? Essentially, it's just a large numerical value that we use to encrypt our data. Imagine, say, ten Rubik cubes, linked together through the center. Every move you make to solve one cube makes the same move on every other cube, each of which have a different initial configuration.

It's theoretically possible to solve all the puzzles together, but it
a) takes quite the computational genius, and
b) takes the computers we have a good deal of time, during which, a handful of cheerful alarms can be set off and security teams can come metaphorically running to intercept and throw out the potential hacker.

That's great, so long as everyone's using the same kind of computer, because it creates an unlikely but usefully level playing field.

The reason quantum computing is expected to be so fast is that it will be able to handle not only comparatively vast numbers of *numbers* simultaneously, but also vast numbers of *computations* simultaneously.

It's likely to look at the intricately constructed mega-puzzle that is pe-quantum public-key encryption,

smile indulgently, say “Cute,” solve the whole thing in the time it takes to say “Cute,” and go about its Wikileaky day, leaving everything that had been protected by public-key encryption exposed to the elements, the hackers, the blackmailers and the hostile nation states.

In theory…

At least, that’s the theory. We don’t technically *know* that quantum computing will be able to do that, and there’s a sense of Millennium Bug planning about the whole thing. But as with Millennium Bug planning, if the nightmare scenario of quantum computing *does* come true and leave everything using public-key encryption open and exposed, we’re going to feel mighty foolish for the half-hour or so before the world dissolves into chaos, anarchy, James Bond movie plots and possibly a primitive non-computer dystopia.

Incidentally, it’s true of course that public-key is only half the story of pre-quantum cryptography. There’s also a private-key element, which is usually individual-specific. But it’s widely considered that if quantum computers can crack public-key cryptography, then private-key is likely to be little more than an *hors d’oeuvres* of decryption, the easy sudoku before it moves on to the cryptic version.

Hence the need to be prepared for the era of quantum computing by deploying post-quantum cryptography. But what *really* is the purpose of post-quantum cryptography? What does it really mean, and perhaps more to the point, how do we really do it? If the giant number-cruncher is coming for all our precious secrets, how in the world do we protect them?

The Science.

Naturally enough, the way post-quantum cryptography works depends on understanding the purpose behind it, and the way the quantum computers are most likely to work.

Behind our folksy, easily digestible Rubik cube analogy, pre-quantum public-key cryptography tends to rely on three hard math problems: the integer factorization problem, the discrete logarithm problem, and the elliptic-curve discrete logarithm problem.

Feel free to look them up if you want to go beyond the Rubik cube analogy. Google will pretend to be your friend.

Post-quantum cryptography, perhaps perversely, will *still* most likely use public-key as its core approach, but will likely focus on any one or more of a handful of other techniques, given that quantum computers are expected to be able to solve the existing security problems in a handful of digital heartbeats, thanks to their ability to rapidly deploy **Shor’s algorithm**.

Potential methods of delivering post-quantum cryptography.

In brief, the front runner *types* of public-key algorithms that are most likely to deliver post-quantum cryptography are:

Lattice-based cryptography.

In particular, it’s worth keeping an eye on NTRU lattice-based cryptography, which has some significant testing behind it (with, admittedly, current computers), and has so far withstood years of attempts to crack it. That’s why NTRU lattice-based cryptography – or at least something called the Stehle–Steinfeld variant of NTRU – is being promoted for study as a potential standard of post-quantum cryptography by the **Post Quantum Cryptography Study Group** sponsored by the European Commission.

Hash-based cryptography.

Less fun than they sound, hash-based cryptographic algorithms have been around since the 1970s (and as such, we might think them useless in fighting 2020s or 2030s quantum computer intrusion). Actually though, their fundamental nature as alternatives to numerical digital signatures might have some skin in the post-quantum cryptography fight. As yet, they're less supported for investigation than the likes of lattice-based cryptography, but there's nothing fundamental that says evolutions of the likes of Lamport or Merkle signatures might not have a part to play in the post-quantum world.

Code-based cryptography.

Another contender favored by the European Commission, code-based cryptographic algorithms tend to rely on error-correcting codes. Ironically, one algorithm called the McEliece signature has withstood attempts to crack it for over 40 years by using random codes. Researchers that have tried to add more structure to the McEliece signature have invariably made it weaker and less stable, suggesting that useful randomness may have a part to play in post-quantum cryptography.

Supersingular elliptic curve isogeny cryptography.

While it might not exactly trip off the tongue, supersingular elliptic curve isogeny cryptography might well prove useful for forward secrecy (useful for avoiding the likes of mass surveillance by unfriendly governments). It's also essentially a quantum-resistant version of an already widely-used version of public-key cryptography, the elliptic curve Diffie-Hellman key, so there are arguments in favor of it being a minimal-hassle upgrade.

Symmetric key quantum resistance.

Another alternative that more or less already exists is symmetric keys. Public-key cryptography is one thing, symmetric key cryptography another, but it's another that already exists and is in use, *and* is expected to be quantum intrusion-resistant. That means there are many organizations suggesting we simply switch out public-key cryptography for symmetric key cryptography altogether.

Whether that will deliver a long-term solution remains as yet hard to judge – at least until we see fully-powered quantum computers, up, running, and on their game. But it's certainly a theoretical way of deferring the problem while robust long-term post-quantum cryptographic algorithms are tested and developed in the field.

Multivariate cryptography.

One of the longer shots in the field right now, multivariate cryptography is exactly what it sounds like – cryptography based on the solving of multivariate equations. In its current form, it's not been particularly effective in testing, and in principle, the idea of essentially making public-key cryptography just a little more complex probably won't survive more than a couple of rounds of evolution of fully-powered quantum computers.

Still, the idea of doing more complex things with existing math appeals in the here and now, and if, for instance, the quantum cryptography apocalypse never arrives in the dramatic fashion that's being forecast, multivariate cryptography might yet have a future as a heightened evolution of pre-quantum cybersecurity.

Whichever options withstand the power of quantum computing best will undoubtedly shape the direction of corporate, government and personal cybersecurity for at least a generation. Which options those turn out to be… we'll have to wait and see. But ultimately, what is the purpose of post-quantum cryptography? It's to make sure business continues as usual in a world of the casual supercomputer in your pock-

et, on your desk, and everywhere else.

15.The Post-Quantum Cryptography Disaster

by Michael P. Fortkort
https://www.einnews.com/pr_news/628455182/the-post-quantum-cryptography-disaster

The Post-Quantum Cryptography algorithm search is at a critical juncture – and it sadly looks like a continuance of the same old mistakes. Current methods result in ever-increasing yearly losses in cybercrime ($6Trillion+), and the dysfunctional algorithm search is going to result in an even worse security disaster.

Here's some evidence:

NIST began a years-long effort to select new Post-Quantum Computing algorithms for standardization in 2016. In July 2022, NIST announced 4 finalists. SIKE, one of the 4 finalists, was immediately broken – using a PC.

"A team of scientists report they were able to defeat one of the post-quantum safe algorithms…and it only took one computational core on a PC working for about an hour." – The Quantum Insider, Matt Swayne 8/5/22

Jao, SIKE co-inventor, on why the weakness surfaced after acceptance by NIST as a finalist:
"It's true that the attack uses mathematics which was [sic] published in the 1990s and 2000s. In a sense, the attack doesn't require new mathematics; it could have been noticed at any time."

So what did NIST do after this fiasco?

"It is perhaps a bit concerning that this is the second example in the past six months of a scheme that made it to the 3rd round of the NIST review process before being completely broken using a classical algorithm. (The earlier example was Rainbow.) Three of the four PQC schemes rely on relatively new assumptions whose exact difficulty is not well understood…" – Jonathan Katz, IEEE, UMd

Even with embarrassing and damning results, NIST's course of action remains unchanged.

Here are the Quantum facts:

- Stronger algorithms are needed because future computers will always be better
- No one knows anything about those future computing capabilities
- That leaves only one PQC algorithm design guaranteed to work and be forever safe under any computing platform – it must not be computationally bound.

Looking for a 'difficult to compute' algorithm (like all of current cryptography) will end up just like SIKE: it looks good until it isn't. And it's not just a matter of finding the math to break it; because if an answer can be computed, it will be found in a future computing real time. So how is looking for the same type of broken things we already have going to solve the problem? Bottom line: it isn't!

But luckily, cryptography already has the answer to this unknown future…and it lies in the past:
There is only one absolute definition of any cryptography that is not computationally bound: Perfect Secrecy

Your immediate reaction is that Perfect Secrecy isn't practical – but here's Claude Shannon:

"It is possible to construct secrecy systems with a finite key for certain "languages" in which the equivocation does not approach zero as $N \to \infty$. In this case, no matter how much material is intercepted, the enemy still does not obtain a unique solution to the cipher but is left with many alternatives, all of reasonable probability. Such systems we call ideal systems. It is possible in any language to approximate such behavior—i.e., to make the approach to zero of $H(N)$ recede out to arbitrarily large N."

Those practical, finite key Ideal Systems are defined as:

"We will define an "ideal" system as one in which $HE(K)$ and $HE(M)$ do not approach zero as $N \to \infty$. A "strongly ideal" system is one in which $HE(K)$ remains constant at $H(K)$."

Turns out there is practical Perfect Secrecy in Shannon Strongly Ideal Systems – all that was required was for someone to create one – and Qwyit has done it. It's forever not computationally bound, meets the real-world definition of Perfect Secrecy (multiple plaintexts encrypting to identical ciphertext), and it delivers 100% safe Cryptography under any Binary, Quantum, AI, or future-unknown computing system.

So why is cybersecurity making all the same mistakes that already cause so many problems – only to be certain that the future is filled with more?

There's no need to find new PQC algorithms: Cryptography already has a universal, forever algorithm: Perfect Secrecy as defined by Shannon and efficiently engineered by Qwyit™ (www.qwyit.com).

16.The Quantum Security Era Is Coming - Here's How Leaders Can Prepare for it

by Michele Mosca and Vikram Sharma
https://www.weforum.org/agenda/2023/04/the-quantum-security-era-is-coming-here-s-how-leaders-can-reap-its-benefits/

When it comes to certain types of complex computational problems – advanced statical modelling in the financial sector, accelerated research and development for pharmaceutical companies or a more efficient supply chain in the automotive industry – quantum computers promise organizations transformative power.

But, for maximum transformative gains, quantum computers must manage a particular risk: the cryptography used to secure many of our daily digital tasks, such as browsing the internet or online banking, will be broken by sufficiently powerful quantum computers.

Recent alarm in the security community around reports that researchers may already be able to break a common type of cryptography on an existing quantum computer reiterates the seriousness of this risk – and how ill-prepared we are if such a report is true.

Furthermore, attackers may already be engaging in Harvest Now, Decrypt Later (HNDL) attacks in which they steal sensitive data today, such as personal health information or military secrets, and retain it until a sufficiently powerful quantum computer arises to break its encryption. If this occurs while the data retains its sensitivity, the consequences could be significant.

Therefore, organizations must act now to understand and prepare to mitigate the risk of quantum computers as soon as possible.

Mitigating cybersecurity risks, embracing the economy of quantum computers

Mitigating the risks quantum computers pose to our cybersecurity infrastructure will require organizations to implement quantum-secure cryptography, elements of which are currently being standardized by the National Institute of Standards and Technology. The European Telecommunications Standards Institute and other organizations are also standardizing other encryption methods, including quantum key distribution.

Similar implementations have shown the process can take many years as cryptography is often deeply embedded in systems with multiple dependencies, including from third parties through the supply chain. Nevertheless, there are several steps leaders can take now before embarking on a more significant transition.

- **Assign responsibility for managing quantum risk within your organization.** Providing someone with a sufficient mandate and resources helps ensure that preparatory steps are taken and is a meaningful first step in understanding your quantum risk.
- **Know what you have to protect and the tools used to protect it.** Creating and managing inventories of sensitive assets and security tools is challenging for any organization. But knowing where and why cryptography is being employed will make it easier to take action to address your quantum risk.
- **Assess your quantum risk.** Define to what extent your organization relies on vulnerable cryptography and to what extent it can effectively manage this cryptography. The results can guide further steps and create awareness across the organization.
- **Include a focus on basic cyber hygiene.** Cryptography is one of many protection mechanisms modern organizations have at their disposal. Organizations should ensure that other cybersecurity measures are effective to partly minimize quantum risk for now and ensure that these measures effectively complement cryptographic solutions.

3 approaches for enabling the quantum transition

Because cryptography is used as a security control in many places throughout systems in organizations, the scope of the transition will be broad and with many dependencies. It is, therefore, essential to start today.

Clear leadership and directive from the board are needed to help executives develop and implement an effective quantum cyber strategy. This engagement should include a consistent review of meaningful key performance indicators to track progress.

Three transition approaches are likely to be adopted by most organizations. The first approach may be combined with either of the other two.

1. **Introduce parallel quantum solutions**

   Managing a parallel implementation is suitable for most organizations if they have sufficient resources. Various cryptographic algorithms publicly available and reviewed are already potentially quantum-safe. Organizations can start using these quantum-secure solutions today in addition to existing classical cryptography, combining their powers.

   There are two major benefits to this approach. First, it provides organizations with a low-barrier opportunity to experiment with implementing quantum-secure cryptography to see what expected and unexpected consequences it may have for their IT systems. This prepares them for when they eventually embark on their complete migration. Secondly, combining quantum-secure and classical cryptography offers a double-layered defence that may protect against today's and tomorrow's threats.

2. **Follow a phased approach**

   Organizations with more complex infrastructure or resource limitations may transition in distinct phases. That means starting with migrating groups of systems to quantum-secure cryptography and having interim "cool-off" periods to define lessons learned to incorporate in the next phase.

   Phase-based transformations allow for investments and milestones to be spread, which can help leaders create support for the migration throughout affected business functions due to less downtime of affected systems. In addition, the continuous adoption of lessons learned from the previous phases and new industry insights (such as developments in the standardization of quantum-secure algorithms) allows for a constant improvement of the quality of the migration.

3. **Complete migration to quantum computers in one go**

   Some organizations, especially smaller or emerging ones, have smaller infrastructure deployments or have limited business needs to communicate sensitive information. These might consider a full overhaul, in which the goal is to become quantum-secure as soon as possible with the knowledge and experience that is currently at hand. Such an approach applies to projects in the early stages of development or deployment of new capabilities.

   A complete "big bang" approach can theoretically provide immediate protection and safeguard against HNDL attacks, which can be valuable for organizations that process very valuable data and may be specifically at risk of HNDL attacks. However, limited preparation and lack of intermittent learning may result in implementation challenges and hamper the longer-term utility of the solution.

Irrespective of the chosen transition scenario, organizations must act now to embrace the quantum era and confidently reap its benefits.

Quantum resilient cryptographic standards and regulatory requirements will be commonplace sooner rather than later. Digital encryption may not yet be broken today but will you be ready when it is?

17.Chinese Quantum Companies and National Strategy 2023

by P Jakob

https://thequantuminsider.com/2023/04/13/a-brief-overview-of-quantum-computing-in-the-us/

Introduction

A BRIEF OVERVIEW OF QUANTUM COMPUTING

Quantum technology is anticipated to revolutionize computing, taking advantage of the world of spooky actions at the subatomic level. It is slated to improve and transform how we conduct large-scale optimization modeling, establish hacking-proof cryptography, and instantaneous communication from entanglement, to name a few. Quantum's uses are undeniable, if not distant. Yet, as progress and discoveries climb the roadblocks, quantum has become one of the hot potatoes states use in their geopolitical tech race. China is no different, prioritizing quantum technology and Chinese quantum companies since 1985 amounting to today being estimated to comprise over 50% of the world's public investment towards quantum.

Similarly, Chinese quantum companies are seen more frequently in the investment portfolios of Chinese VCs and angel investors, offering promising opportunities for the future. In this area, private investment is more than doubling each year from predominantly domestic private investors.

This article will uncover the difficult-to-attain information from inside the Middle Kingdom, China, shedding light on the nation's public spending and private investments landscape of quantum computing. The metrics, data, and insights which made this article possible came from the bespoke Quantum Insider Intelligence Platform and the premium report which delves into greater detail on the points made.

CHINA'S ROLE AND INVESTMENTS IN THE QUANTUM TECHNOLOGY MARKET

We are amidst a 21st-century technology race between the West and China. A competition not on space exploration but on emerging technologies such as AI and quantum.

The rising tensions between China and the US with geopolitical risks straining global supply chains have prompted China to seek technological sovereignty in advanced semiconductors, quantum technology, AI, and more.

As a result, China has increased its state funding to an estimated (but highly disputed) >$15 billion[1] in quantum research and advancement with its assorted applications from security to defense to AI.

Comparably, the recently announced 10-year plan to progress and commercialize quantum in the UK was £2.5bn ($3.125bn) from the £1bn allocated in 2014. Further, the Chinese state funding is double the committed total across the EU for quantum and four times that of the US.

Here are two shining examples of where the Chinese national spending and policy focus on quantum goes:

- The world's largest quantum research facility in Hefei, Anhui Province, a 37-hectare National Laboratory for Quantum Science.
- The Chinese scale-up Origin Quantum attained $148m in Series B funding led by the state-owned venture fund Shenzhen Capital.

It goes without saying China is one of the global leaders in quantum, presenting opportunities for foreign

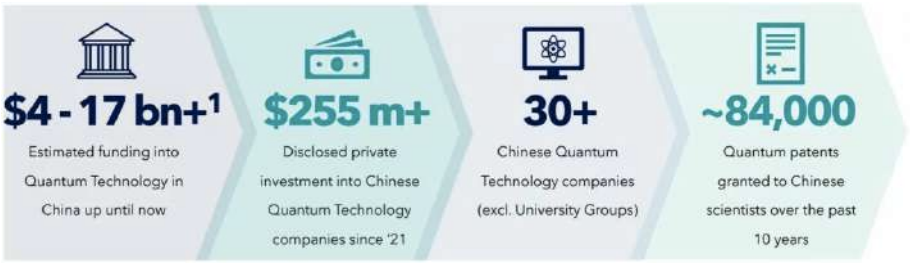
[1] It is difficult to accurately calculate and estimate China's subsidizing and state investment in quantum due to lacking information availability and reliability.

investment and demanding attention from policymakers.

China's Quantum Computing Market

OVERVIEW OF CHINESE QUANTUM COMPANIES

In one snapshot, this is China's quantum strategy and market:



Breaking down the Chinese quantum companies by segment reveals significant growth in quantum computing, despite the nation's leading role in quantum communications and quantum dots. See the pie chart below.

GOVERNMENT INITIATIVES AND INVESTMENTS IN QUANTUM COMPUTING

The difference between the quantum investment market of the US to China is the different economic models underpinning the two nations. China has significantly higher public spending beyond simply R&D compared to the US. Whereas private investments in quantum technologies, research, and startups are substantially higher in the US than in China.

Here are the differences in four points:

- China's public spending on quantum is four times higher than the US.
- US private investment in quantum is over 1350% higher than in China.
- There are over 10x the number of quantum startups and 6x quantum investors in the US to China.
- Interestingly, China holds over 30% quantum patents than the US. However, the patents resided in the US are accredited in globally respected journals for their scientific impact and innovation.

To venture outside the Pax Americana perspective, public spending in the UK comprises almost 0.12% of FY21 GDP with $4.4bn, 0.07% in Germany with $3bn and France with $2.2bn, and the pan-European Quantum Flagship initiative of 0.01% of GDP with $1.1bn.

In either case, China accounts for over 50% of the estimated global public investment in quantum allocated to research and Chinese quantum companies.

Because of the rising adversarial relationship between the US and China, the US is turning protectionist in its policies and national strategy. In August of last year, the signed CHIPS and Sciences Act aims to compete with China's increasing focus and state funding towards advanced semiconductor sovereignty and Chinese quantum supremacy. The Act comprises $280 billion of spending to support advanced semiconductor research, advancement, and domestic manufacturing with emerging technologies such as quantum[2]. Furthermore, the Dutch imposed a trade restriction with China under US pressure, barring access to their Advanced Semiconductor Materials Lithography (ASML)[3].

These external factors and the geopolitical tech race will further spur China's state and private spending with favorable policy incentives toward quantum technology and Chinese quantum companies. In other words, presenting opportunities for quantum investors and the attention of policymakers.

CHINESE QUANTUM ACHIEVEMENTS

China is one of the leading international players in quantum technology. To keep the cold war analogy motif, China became the first to launch a quantum-enabled satellite named Micius which some referred to as the 21st-century Sputnik. A quantum breakthrough that established an over 4,600 km quantum communications network between Shanghai and Beijing, comprising quantum radars and quantum decryption. We will circle back to this as a case study.

Further, a year after Google AI Quantum announced the capabilities of the Sycamore quantum computer achieving 53 Qubits with a declaration of quantum supremacy (a significant quantum advantage over traditional supercomputers), China announced they leapfrogged Google with two quantum computers named Zuchongzhi (superconductor quantum computer) and Jiuzhang 2.0 (photonic quantum computer), the former claiming 66 Qubits (although in demonstration achieved 58 Qubits).

A FOCUS ON CHINESE QUANTUM EDUCATION

Following the historical precedent, China's policy changes obey a five-year plan, and as such, the latest 14th five-year plan from 2021 announced quantum technology as one of the key pillars of the Chinese technology sovereignty and Chinese quantum supremacy goal. Yet, becoming a leader in quantum technology is no easy endeavor with a high demand for educated white-collar labor.

Because of this, two Chinese education reforms titled the "Education Modernisation 2035 Plan" and the "Implementation Plan for Accelerating Education Modernisation" were set in place. Two legislative initiatives aiming to prepare the future Chinese for a quantum future funded by about 4% of the Chinese GDP, approximately $150-200bn yearly. While as a supporting measure, the Chinese state, since 2008, also encouraged student repatriation at leading Western universities.

Besides public schooling, Chinese quantum companies such as Origin Quantum, CIQTEK, and Alibaba have established in-house quantum education while frequently interacting with universities down to pri-

---

[2] Badlam J, Clark S, Gajendragadkar S, Kumar A, O'Rourke S, Swartz D. The CHIPS and Science Act: Here's what's in it. McKinsey Co 2022:7. https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-chips-and-science-act-heres-whats-in-it.

[3] Sterling T, Freifeld K, Alper A. Dutch to restrict semiconductor tech exports to China, joining US effort. Reuters 2023:4. https://www.reuters.com/technology/dutch-responds-us-china-policy-with-plan-curb-semiconductor-tech-exports-2023-03-08/.

mary schools, sparking an interest in quantum technologies.

THE CHINESE QUANTUM BUSINESS ENVIRONMENT

Over 30 key quantum companies are active in China, spanning large tech conglomerates like Alibaba with Quantum Computing as a Service to startups like TuringQ developing optical quantum computer chips.

However, four key business figures behind the Chinese quantum environment are worth noting:

- **Pan Jianwei,** known as the "Father of Quantum"
- **Guo Guangcan**, the pioneer of quantum optics
- **Guo Guoping,** Origin Quantum founder
- **Jin Xianmin**, TuringQ founder

Four respected figures within quantum in China you can discover more about in the premium report this article is based on "Quantum Technology in China 2023 Review", for their roles, legacy, and position within the Chinese quantum landscape.

The Chinese Private Quantum Investment Landscape

While the private investment environment for quantum in China is significantly smaller than its state spending, investments are rapidly growing.

By and large, quantum investments are centered around Pre-seed/Seed, Series A, and Series B of private quantum businesses. In 2021, $62m was invested into quantum startups, with over two-thirds classified as Seed funding. The following year, 2022, this investment figure more than tripled with $194m invested, with over two-thirds being Series B funding and the rest Series A. Likewise, 66% of these private investments went to Superconducting Quantum Computers, 31% to Photonics, and only 3% to Trapped Ion.

Here are three examples.

Three Case Studies: Quantum Computing Success Stories in China

ALIBABA QUANTUM COMPUTING AS A SERVICE

Active in quantum since 2015, Alibaba is a diversified tech conglomerate. The corporation today operates its own Quantum Lab Academy teaching employees and students about the prospects of quantum computing. Whereas Alibaba Quantum Laboratory is a full-stack R&D service offering an 11-qubit quantum cloud platform. Alibaba, to date, has reportedly further invested over $15bn into emerging technologies such as quantum (based on limited rumours).

ORIGIN QUANTUM'S SOARING RISE IN QUANTUM TECHNOLOGY

Origin was founded in 2017 and is a successful scaleup that offers quantum simulation in upskilling and training quantum computing developers. Origin further manufactures a two-qubit chip based on quantum dot technology and a six-qubit chip using superconducting. The scaleup has accrued a total of $163m and is ranked number six for total quantum patents globally, with the latest development of delivering a 24-qubit superconducting quantum computer.

THE CHINESE BREAKTHROUGH IN A SATELLITE QUANTUM COMMUNICATION NETWORK

Marked as the Sputnik of the 21st century. In 2016, the Chinese defied reality by launching the first quantum satellite establishing a quantum communication network using entanglement to communicate instantaneously between Xinjiang Ground Station, Delingha Ground Station, and Ali Observatory. The quantum satellite Micius has since achieved entanglement-based quantum-key distribution, allowing for fully secure and encrypted communication.

The ultimate aim is to use this technology to achieve a secure quantum-based internet. As the latest announcement, in 2021, China accomplished the world's first integrated quantum communication network from over 700 optical fibers with two ground-to-satellite links using quantum key distribution (QKD).

In conclusion

Driven by its national strategy to attain technological sovereignty and quantum supremacy in AI, quantum, advanced semiconductors, and more. China's state funding in quantum research and improvement comprises over 50% of the world's public spending on quantum. This considerable state focus on quantum has propelled China to be a global leader in pioneering and advancing a spanning quantum communications network and constructing the largest quantum research facility in the world.

So despite the significant disparity between China's private investment landscape lacking behind the US, it is expanding at an unprecedented pace every year with an increasing number of startups and scale-ups further nurtured by large tech conglomerates like Alibaba.

Overall, China's rapid advances in quantum technology, combined with significant state funding and increasing private investment, have positioned it as a major player in the global quantum market, presenting opportunities for foreign investors and policymakers to take note of the nation's undeniable achievements.

If you want a detailed picture of China's quantum market, investment landscape, opportunities, and more, check out the premium report: Quantum Technology in China 2023 Review.

18.A Brief Overview of Quantum Computing in the US

by James Dargan
https://thequantuminsider.com/2023/04/13/a-brief-overview-of-quantum-computing-in-the-us/

Introduction

Overall, the US is one of the leading players in the research, investment and private sector in quantum tech globally. Going back a few decades, the US was the dominant player until China made strides, beginning in the 2010s. With a handful of research institutes, many universities and a healthy number of corporates and startups, this is only set to continue.

The Quantum Insider must warn you, however, that as it says in the title, this is a *"brief"* outline of the quantum tech industry in the US, and we have only covered a small fraction of what is actually going on. If we missed anyone or anything, please don't take it personally—we're only human, after all.

Government Position

The US government has made a number of strategic investments in quantum computing (QC) research and development through various initiatives, the most important in recent times being the National Quantum Initiative Act, signed into law in 2018 by President Donald Trump and coordinated by The National Quantum Coordination Office. The Act provides the United States with a plan to advance quantum technology, particularly quantum computing and offers general support for a number of government agencies that develop programs connected to quantum science and technology in the country.

Prior to that, however, the US government was the first to conduct a workshop on quantum computing organized by NIST in 1994. Two years later, it issued the first public call for research proposals in quantum information processing in a joint partnership with the Army Research Laboratory.

Research

The government's investments in QC research are aimed at advancing this technology to solve some of the most challenging problems in science, engineering and national security. Research is currently aimed at applying quantum computing technology to improve outcomes in drug discovery and cryptography, as well as financial and climate modelling.

A report by The Quantum Insider published in January of this year, states that as part of its commitment to accelerating U.S. leadership in QIS, the Biden-Harris Administration has emphasized a whole-of-government and whole-of-society approach while mitigating potential risks. Additionally, with budget expenditures for QIS R&D increasing from $449 million in 2019 to $918 million in 2022, and requested budget authority of $844 million for 2023, the United States has made substantial and sustained investments in QIS R&D.

The government has also established several national laboratories whose sole focus is targeted at quantum computing research. These include the Argonne National Laboratory, whose CELS Directorate is pursuing research in quantum information science that spans theory, algorithms, simulations, and modelling of quantum systems, the Brookhaven National Laboratory, which is delivering a cross-disciplinary strategy to harness quantum effects in physics for advanced computing, communications, and fundamental science and the Lawrence Berkeley National Laboratory, busy researching theory to application for quantum tech.

Many private institutions are researching QC too, some of the best include MIT, Caltech, Harvard, and Stanford.

Private Sector

Here is where the US really dominates, with several leading quantum computing companies, many of them leading corporations from the classical computing industry. Examples of these such as IBM and its research and production of superconducting circuit-based commercial quantum computers. Google comes to mind and its 53-qubit superconducting Sycamore quantum processor, created by Google's Artificial Intelligence division. Microsoft is another major player on the market, featuring solutions, software and hardware delivered through Azure.

Independent startup players — and there are a lot of them — include IonQ, a publicly-traded spinoff from the University of Maryland and Duke University. The company is developing a general-purpose trapped ion quantum computer and software to generate, optimize and execute quantum circuits. Another to note is Quantum Computing Inc. The Leesburg, Virginia-based company delivers a suite of full-stack quantum solutions that include the Entropy Quantum Computer (EQC), designed to exclude noise in the system and create useful qubits to perform computations and its software offering Qatalyst, a cloud-based service that solves different types of optimization problems on a variety of quantum computers or quantum simulators that is also a public company.

Key People

Although it would be nearly impossible to mention the most important people currently involved in quantum tech in the country here as it is a very long list, two that stand out are John Martinis and John Preskill.

Martinis' influence spans both academia and the commercial sector. A professor of physics at the University of California, Santa Barbara, In 2014 he joined the Google Quantum A.I. Lab in order to build a quantum computer using superconducting qubits, though he resigned from Google in 2020 and moved to Australia to join Silicon Quantum Computing, a startup founded by Professor Michelle Simmons, which he was involved in until 2021.

2019 was an important year academically for Martinis, as he and his team published a paper in Nature, *Quantum supremacy using a programmable superconducting processor*, where they presented how they achieved quantum supremacy (hereby disproving the extended Church–Turing thesis) for the first time using a 53-qubits quantum computer.

Another notable figure is John Preskill, an American theoretical physicist and the Richard P. Feynman Professor of Theoretical Physics at the California Institute of Technology, where he is also the Director of the Institute for Quantum Information and Matter.

Preskill is known to have coined not one but two terms that are common parlance in quantum computing circles today, *"quantum supremacy"* back in 2012 and *"noisy intermediate-scale quantum"* (NISQ) in 2018.

Conclusion

It's guaranteed the US will be a leader this decade and beyond in quantum tech, spurred on by significant government investment in research and a thriving private ecosystem.

Quantum Intelligence Platform

This is only a basic overview of what is happening in the US in the quantum tech industry. Want to find out more about the US quantum ecosystem? For a more in-depth look at the market there, look no further than The Quantum Insider's very own Quantum Intelligence Platform, the leading provider of Quantum Computing market data, reports, analytics, and insights on QC companies, investors, funding, and more.

Based on our proprietary taxonomy and customizable metadata, the platform allows you to find robust funding commercial information that can be filtered by subsector and technology type while being effortlessly integrated into The Quantum Insider's database of news and information on the Quantum Computing industry.

But that's not all, recently we added our Data Graph Explorer, a tool that allows those interested to spot interesting relationships and connections in the quantum market and make decisions based on those relationships.

19.Quantum Collaboration: Indian Navy

Teams up with Raman Research Institute

by PBNS
https://newsonair.com/2023/04/12/quantum-collaboration-indian-navy-teams-up-with-raman-research-institute/

The Indian Navy is set to collaborate with the Raman Research Institute (RRI) to develop secure maritime communications using quantum technology. The MoU between RRI, an autonomous institute of the Department of Science and Technology (DST), and the Weapons and Electronics Systems Engineering Establishment (WESEE), the R&D establishment of the Indian Navy, was signed for a period of five years. The RRI's Quantum Information and Computing (QuIC) lab will lead the research efforts towards developing quantum key distribution techniques that the Indian Navy could leverage in the nation's efforts towards securing free space communications.

A landmark collaboration

The Director of RRI, Professor Tarun Souradeep, expressed his excitement about the partnership, stating, "I am absolutely delighted that Indian Science and Technology ecosystem has been opening borders in recent years that enable talented and world-class researchers in the academic research institutions to contribute to the growth of Science and Technology capabilities in strategic areas of national importance." The collaboration between RRI and WESEE will enable cutting-edge research towards identifying potential maritime use-cases for the Indian Navy.

The QuIC lab's expertise in secure quantum communications

The QuIC lab has been leading India's research in the field of secure quantum communication. Some of its significant achievements include the development of an end-to-end simulation toolkit named "qkdSim", establishing secure communication between two buildings, and, more recently, between a stationary source and a mobile receiver. The QuIC lab also happens to be India's first laboratory to propose and implement a wide range of applications using single and entangled photons, particularly towards establishing secure communications in strategic areas like banking, defence, and cyber security.

Looking forward to a secure future

The collaboration between RRI and WESEE is expected to enable the Indian Navy to leverage quantum technologies for secure maritime communications. The partnership between RRI and WESEE will create a robust platform to identify potential use cases for quantum key distribution techniques. With the QuIC lab's expertise in secure quantum communication, this partnership is poised to enable cutting-edge research towards securing free space communications in the maritime domain.

20.A Brief Overview of Quantum Computing in Germany

by James Dargan
https://thequantuminsider.com/2023/04/11/a-brief-overview-of-quantum-computing-in-germany/

Introduction

Germany has a strong presence in the field of quantum computing, with several universities, research institutions and companies actively pursuing research and development in this area, having built on its reputation for more than a century of fine academic work in quantum mechanics. It is clear, from this, that Germany will be a leading player in the years to come.

The Quantum Insider must warn you, however, that as it says in the title, this is a *"brief"* outline of the quantum tech industry in Germany, and we have only covered a fraction of what is actually going on. If we missed anyone or anything, please don't take it personally—we're only human, after all.

Government Position

In 2018, the German Federal Government announced a Framework program to bring quantum technologies to market while also allocating €650 million in funding to its quantum technologies program. The purpose of the program is to establish the framework conditions to prepare for new economic opportunities and markets. Additionally, two years later the German government announced a €2 billion quantum initiative, adding to the EU's intentions for €1 billion in investment in the sector until 2028.

The German government has also established several research institutions and centres of excellence dedicated to quantum computing and related fields. For example, the Fraunhofer Society has established the Fraunhofer Institute for Applied and Integrated Security (AISEC) to focus on research in quantum cryptography and other aspects of quantum security.

Another of note is The Max Planck Institute of Quantum Optics (MPQ), one of the world's leading research institutions in quantum optics and quantum information science.

Germany also paid for a quantum computer from IBM (a Quantum System One computer) in 2021. This was IBM's first quantum computer outside of the US and is also now one of the most powerful in Europe.

In 2022, an order worth €208 million was made by the German Aerospace Center (DLR) for ion trap-based quantum computing, issued as part of the DLR's Quantum Computing Initiative. Some €740 million is to be provided by the Federal Ministry for Economic Affairs and Climate Action to assist the project. Around 80% of this funding, approximately €600 million, is being used for research and development contracts with companies for various variants of quantum computers, with the rest going to DLR's own research.

In addition, the German government has invested in the development of quantum computing hardware and software, with a particular focus on building a strong ecosystem of startups and small and medium-sized enterprises (SMEs) in the field.

Overall, the German government is committed to maintaining its position as a leader in the global race for quantum technology, including quantum computing, and is actively investing in research, development and commercialization in this field.

Research

Germany has been active in the field of quantum computing research for several decades, and the country can boast several world-class research universities involved in quantum computing research in Germany.

The Technical University of Munich is one such establishment, having a strong research program in

quantum computing, including a focus on the development of quantum algorithms and software, quantum communication, and quantum cryptography.

The University of Cologne is another. It has a research group dedicated to quantum computing, specializing in the development of new quantum computing hardware and the exploration of the fundamental principles of quantum computing.

Let's not forget about The University of Hannover either, whose research group is focused on the development of quantum computing hardware and the development of new technologies for quantum information processing.

In addition to these institutions and research groups, there are also several companies in Germany that are involved in quantum computing research, including the already mentioned IBM, Google, and Microsoft. These companies have established research partnerships with universities and research institutions in Germany to advance the development of quantum computing technology.

Private Sector

The European multinational aerospace corporation Airbus has a research group in Germany that is exploring the potential applications of quantum computing in the aerospace industry.

In the startup world, Germany has several companies developing interesting IP in quantum technologies. The companies below are a sample and represent a non-exhaustive list:

- eleQtron, founded in 2020 and based in Siegen, develops and operates quantum computers based on trapped ions. Its intermediate-scale quantum processors are designed to be optimized for near-term industrially relevant quantum applications.

- Founded in 2018 and based in the city of Karlsruhe, HQS Quantum Simulations (formerly Heisenberg Quantum Simulations) provides software for material scientists in the chemical industry and academia that incorporates sophisticated quantum-level models of the properties of molecules and materials, giving researchers deeper insights they need to identify the perfect solution.

- Qruise was founded in 2021 and based in Saarbrucken, the startup develops software that helps scientists and researchers use Machine Learning (ML) tools in their day-to-day scientific workflows without having to worry about what's under the hood.

Key People

Like other countries, Germany has its fair share of luminaries in the industry. Here are a couple of the key people working in the German quantum ecosystem:

One such expert is Christian Pfleiderer, a Scientific Advisor and co-founder of kiutra, a German startup developing next-generation cooling devices for basic research, quantum technology and detector applications.

Pfleiderer holds the chair for Topology of Correlated Systems at TUM and has more than 30 years of experience in low-temperature science at various research institutes worldwide.

Jens Eisert is a professor of Quantum Physics at Freie Universität Berlin, on the Scientific Advisory Board at quantum company Zapata Computing.

Eisert is known for his research in quantum information science and quantum many-body theory in con-

densed matter physics, making significant contributions to entanglement theory and the study of quantum computational models, as well as quantum optical implementations of protocols in quantum technologies and the study of complex quantum systems.

Another important person in quantum in Germany is Reinhard Ploss, a representative of Quantum Technology & Application Consortium (QUTAC), the German quantum tech consortium. Ploss was awarded his doctorate in engineering in 1990. In 2007, Ploss was appointed to the Management Board of Infineon Technologies AG, where he was responsible for Operations. He subsequently held the position of Chairman and CEO from 2012 until 2022.

Ploss has chaired the Supervisory Board of Knorr-Bremse AG since May 2022.

Conclusion

Overall, Germany is well-positioned to be a strong player in the development of quantum computing technologies, with a strong research infrastructure and a highly skilled workforce.

Quantum Intelligence Platform

This is only a basic overview of what is happening in Germany in the quantum tech industry. Want to find out more about the German quantum ecosystem? For a more in-depth look at the market there, look no further than The Quantum Insider's very own Quantum Intelligence Platform, the leading provider of Quantum Computing market data, reports, analytics, and insights on QC companies, investors, funding, and more.

Based on our proprietary taxonomy and customizable metadata, the platform allows you to find robust funding commercial information that can be filtered by subsector and technology type while being effortlessly integrated into The Quantum Insider's database of news and information on the Quantum Computing industry.

But that's not all, recently we added our Data Graph Explorer, a tool that allows those interested to spot interesting relationships and connections in the quantum market and make decisions based on those relationships.

21.What Is The Price of a Quantum Computer in 2023?

by James Dargan
https://thequantuminsider.com/2023/04/10/price-of-a-quantum-computer/

The quantum computer has become the focus of much attention in recent years as it has the potential to revolutionize computing. Quantum computers are incredibly powerful, and their applications range from data encryption and analysis to artificial intelligence and machine learning. However, due to their complexity, quantum computers cost a significant amount of money – but exactly how much?

In this article, we'll explore the current prices of quantum computers and provide some insight into why they're so expensive.

What Are Quantum Computers & What Makes Them Worth It?

In contrast to classical computers, quantum computers rely on quantum mechanics to perform calculations, manipulating quantum bits (qubits) in order to represent information.

Qubits are fundamentally a two-state quantum-mechanical system. This phenomenon is called superposition and allows quantum computers to carry out specific calculations at a much faster rate than classical computers.

Quantum computers, we must note, have the potential to perform certain tasks like factoring large numbers or searching large databases for specific information sometimes better than classical models.

One more unique feature of quantum mechanics that quantum computers possess that classical computers do not is entanglement. This is where two or more qubits become connected (entangled) and their states become reliant on each other, which makes it possible for quantum computers to execute operations on multiple qubits simultaneously. This — like superposition — allows quantum computers to figure out specific problems exponentially faster than classical computers.

Quantum computers are currently at the entry stage of their development. Companies like Microsoft, Google and IBM (and many startups too) — as well as dozens of universities and government research institutes — are researching, developing and manufacturing early NISQ models whose applications will hopefully have far-reaching effects for optimization and logistics, simulating complex systems for molecular chemistry and cryptography problems.

What Types Of Quantum Computers Exist?

2023 sees several types of quantum computers being developed and manufactured. These are typically divided into the qubit modality that they are leveraging. **Currently, there are five leading qubit-type approaches**. There are:

- **SUPERCONDUCTING**

  Superconducting qubit quantum computers are the most widely used type of quantum computer. These types of quantum computers utilize minute electrical circuits to produce and ultimately manipulate qubits, which are usually made of superconducting materials.

  Currently, companies working on this qubit modality include organizations such as Google, IBM, Microsoft, Rigetti Computing, IQM, and Quantum Circuits, Inc.

- **TRAPPED IONS**

  Another popular approach is by using ion trap quantum computers. These utilize atoms or molecules with a net electrical charge called “ions” that are trapped and manipulated using electric and magnetic fields to store and process quantum information.

  Companies developing quantum computers in this field include organizations such as Quantinuum (formed after a merger of Honeywell Quantum Solutions and Cambridge Quantum Computing), ionQ, Alpine Quantum Technologies, and eleQtron.

- **PHOTONIC**

  Another important qubit approach that has supporters is photonic quantum computers. These use photons (particles of light) to carry and process quantum information.

Commercial players representing this qubit modality include organizations such as PsiQuantum, Xanadu and ORCA Computing.

- **NEUTRAL ATOMS**

  Neutral atoms quantum computing utilizes In a neutral-atom quantum processor, which are atoms suspended in an ultrahigh vacuum by arrays of tightly focused laser beams called optical tweezers. Researchers have scaled up to arrays of more than 100 alkali atoms, each of which has one valence electron, and executed quantum algorithms using smaller arrays.

  Commercial players here include such organizations as ColdQuanta, QuEra and Pasqal.

- **QUANTUM DOTS**

  Quantum dot quantum computing utilizes qubits made up of pairs of quantum dots, which are silicon qubits. These properties make them attractive for a variety of applications, including use in quantum computers.

  Companies invested in this approach include organizations such as Diraq, Intel and Quantum Motion.

- **OTHER QUBIT MODALITIES**

  There are also several other approaches such as electrons on helium, quantum computers that use silicon CMOS and nitrogen-vacancy centers (also known as N-V centres).

It's worth taking into consideration before jumping to conclusions that each type of quantum computer has its unique advantages and disadvantages and that different types of quantum computers may be better suited for different types of problems.

Can You Buy a Quantum Computer?

Yes, it's possible to buy a quantum computer in 2023. However, quantum computers are not yet widely available to the general public and are currently very expensive and extremely difficult to manufacture. Another stumbling block to consider is the majority of these machines are owned or operated by large corporations, research institutions and government bodies, so access to them (never mind purchasing one) depends on the access terms of these commercial enterprises and institutions.

If, however, an individual (or company, for that matter) were somehow interested in buying a quantum computer, the best way to approach this would be to contact the likes of IBM, Microsoft, Rigetti Computing, D-Wave or Google directly. They can offer individuals access to their quantum computing resources through cloud-based services, allowing researchers, developers, and businesses to experiment with and utilize quantum computing power without owning the physical hardware. The cost of using these services can vary depending on the amount of time and resources used but typically ranges from a few dollars to several thousand dollars per hour.

Quantum Computer Prices in 2023

As already mentioned, quantum computing is a technology that is quickly advancing but is still in its early stages. The caveat is that putting a price on such a machine is more an art form, rather than a science. Things to consider before the hypothetical purchase of a quantum computer is made could be what type of system you want to purchase, the number of qubits required and—*another important thing*—the level of expert support required from the vendor when using the machine. All these things will have

an influence on the overall cost.

To give you some estimate, The Verge quoted it would cost some $15 million dollars to purchase the D-Wave 2000Q quantum computer, though the article was from way back in 2017 and prices—as well as inflation—have risen considerably since then.

As a ballpark figure, the cost of buying a full machine as of 2023 is currently very high, with the kit that goes into most systems costing hundreds of thousands of dollars. Quantum computing systems like IBM are sold for tens of millions as part of full-service contract over several years.

For example, Microsoft's Azure quantum computing cloud-based service allows first-time users $500 dollars worth of free Azure Quantum Credits for use with each participating quantum hardware provider. They report that if you have used up all the credits and require more, you can apply to the Azure Quantum Credits program.

Another provider of quantum computers is AWS, whose pricing plans to use its cloud-based service start at $29 per month and include AWS Support.

For a more detailed look at the pricing of both Microsft and AWS quantum computer services, go to the links here and here.

Quantum Computer Cost Forecast

Many experts in the industry predict the cost of quantum computing hardware will continue to decrease over time as the technology advances, making it more accessible to a broader range of businesses and organizations. In a recent talk, the CTO of the CIA Nand Mulchandani noted that the quantum industry is still very early and unit costs are still very high, as we are very much in the research and development stage.

In general, quantum computer prices are sure to be influenced by several important factors, including how advanced discoveries in the sector are made, market demand for the technology and competition among quantum computing providers.

Will Quantum Computers Reach Commercial Usage Soon?

Again, this question requires a crystal ball to predict accurately, but as things stand quantum computers are a promising technology that could revolutionize various fields, including machine learning, optimization and material science.

Considering this, the most technologically advanced quantum computers currently by the likes of IBM and Google have hundreds of qubits, which is a great thing in and of itself. However, to really get to where we want to be with the technology, qubit numbers may need to increase significantly, to perhaps thousands or even millions of qubits to have any useful impact in the commercial sphere.

Furthermore, these machines require complex infrastructure and cooling systems (in many cases, see superconducting quantum computing) to maintain the required low temperatures for the qubits to function properly, as well as reliable error correction systems.

Despite these challenges, we are slowly getting there as an industry. While it is difficult to precisely predict the timeline for when quantum computers will reach commercial usage, many experts believe that practical applications may emerge within the next decade or two.

Conclusion

The Quantum Insider observes with a keen eye the market trends and technological narrative that is evolving as we speak. When thinking about the price of a quantum computer in 2023, it's worth considering the access method, the type of computer and usage requirements.

22.A Brief Overview of Quantum Computing in France

by James Dargan
https://thequantuminsider.com/2023/04/07/a-brief-overview-of-quantum-computing-in-france/

Introduction

France has a solid background in developing and researching quantum computing and quantum tech. With world-class research institutes and government agencies, the country is one of the leaders on the European continent and on the world stage for quantum innovation.

The Quantum Insider must warn you, however, that as it says in the title, this is a *"brief"* outline of the quantum tech industry in France, and we have only covered a fraction of what is actually going on. If we missed anyone or anything, please don't take it personally—we're only human, after all.

Government Position

In early 2021, French President Emmanuel Macron announced his country intended to build a "quantum plan" for France worth about 1.8 billion euros over the following five years. Since then, the country has been busy. Only last December, Macron announced the sending of the "first diplomatic telegram encrypted using post-quantum cryptography" to the French embassy in Washington, a clear signal that France is serious about PQC and other areas of quantum tech.

In the same month, France agreed to deepen collaboration with the US on quantum information science, part of the earlier Agreement on Science and Technology Cooperation the two countries signed in 2018 and the Joint Statement on Science and Technology Cooperation signed in 2021.

Research

The Institut Quantique (IQ), a joint research institute between the Université de Sherbrooke in Canada and the Université Grenoble Alpes in France, focuses on quantum computing, quantum communication and quantum materials.

CEA-Leti, whose research institute is located in Grenoble, has a research program on quantum computing, including research on superconducting qubits and quantum simulation.

Others include the École Polytechnique — The Theoretical Physics Center (CPHT), based in Palaiseau, Loria — Classical and QUAntum MOdels of Computation (MOCQUA) and Sorbonne Université and its Quantum Information Center.

Private Sector

France has a thriving quantum private sector, with over a dozen startups in the space. Here is a sample:

Pasqal was founded in 2019 and is building a programmable quantum simulator using atomic arrays of neutral atoms.

Alice & Bob is a company working towards building an error-corrected, fault-tolerant quantum computer.

Quandela is yet another one. The Paris-based startup is developing high-performance devices for quantum optics applications.

On the financial side of things, venture capital firm Quantonation specializes in quantum technologies by investing in startups working on quantum computing, quantum communication and quantum sensing.

Although a publicly traded company, the French multinational Thales Group specializes in electronics and defence but now has a quantum research program that focuses on quantum cryptography and quantum sensing.

Key People

Here are a couple of the key people working to make the French quantum ecosystem one of the best in the world:

Alain Aspect is a physicist known for his experimental work on quantum entanglement. For this, he was awarded the 2022 Nobel Prize in Physics, jointly with John Clauser and Anton Zeilinger, “for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science”. Aspect is Augustin Fresnel Professor at Institut d’Optique Graduate School, France, Professor at Ecole Polytechnique, France, Senior Fellow of the Institute of Advanced Studies and adjunct professor at City University, Hong Kong, and Distinguished scientist.

Along with this, Aspect is also involved on the commercial side of things, as he is a co-founder and scientific advisor for Pasqal.

Another individual making quantum more accessible is Christophe Jurczak, founder and partner at Quantonation, Treasurer and a Director at The Unitary Fund — a non-profit helping create a quantum technology ecosystem that benefits the most people—as well as acting as a Mentor at Duality Accelerator, an accelerator supporting next-generation startups focused on quantum science and technology. Jurczak is also on the board at quantum startup, Welinq, which provides a high-performance quantum memory to deploy our hardware-agnostic and full-stack quantum links solution in order to interconnect multiple quantum processing units.

Conclusion

It’s clear France has a strong presence in global quantum computing. With top-class research institutes, a plentiful supply of startups, venture capital firms, and corporations all contributing to the development of quantum technology, the country is set to play an important role in the future.

For further reading on France’s quantum tech landscape, please check out our French National Quantum Update, published monthly and this detailed report here. Additionally, on June 13th the France Quantum conference takes place at Station F, Paris.

Quantum Intelligence Platform

This is only a basic overview of what is happening in France in the quantum tech industry. Want to find

out more about the French quantum ecosystem? For a more in-depth look at the market there, look no further than The Quantum Insider's very own Quantum Intelligence Platform, the leading provider of Quantum Computing market data, reports, analytics, and insights on QC companies, investors, funding, and more.

Based on our proprietary taxonomy and customizable metadata, the platform allows you to find robust funding commercial information that can be filtered by subsector and technology type while being effortlessly integrated into The Quantum Insider's database of news and information on the Quantum Computing industry.

But that's not all, recently we added our Data Graph Explorer, a tool that allows those interested to spot interesting relationships and connections in the quantum market and make decisions based on those relationships.

23.Future of Quantum Computing: Unlocking The Possibilities

by James Dargan
https://thequantuminsider.com/2023/04/06/future-of-quantum-computing/

The future of quantum computing is here. As quantum computing develops quickly, it will have a major impact on the future of computing. A quantum computer could transform the way we think about computing, increasing processing speeds exponentially and granting access to previously inaccessible data.

Is Quantum Computing the Present or Future?

Quantum computing is both the present and the future. Unlike classical computing, which uses bits to represent data and perform operations, quantum computing uses qubits (quantum bits), which can exist in multiple states that are probabilistically determined, known as superposition. This will allow quantum computers to perform certain types of calculations much faster than classical computers.

While it is still an emerging technology, there have been significant advancements in the field in recent years. Quantum computers have already been built and are being used by researchers and companies for various tasks, such as optimization problems and simulation of quantum systems.

However, quantum computing is still in its infancy, and there are many technical and practical challenges that need to be overcome before it becomes a mainstream technology. These challenges include improving the stability and scalability of quantum hardware, developing better algorithms and error-correction techniques, and finding new applications that can take advantage of quantum computing's unique properties.

What Does The Future Of Quantum Computing Hold?

Quantum computing is a rapidly developing field, and its future is full of exciting possibilities. Several potential directions for quantum computing in the future are listed below:

1. **IMPROVED HARDWARE**

   Developing hardware that can reliably perform quantum computations is one of the main chal-

lenges in quantum computing. In order to mitigate the effects of noise and decoherence, researchers are developing better quantum processors and improving error correction techniques.

2. **APPLICATIONS IN CHEMISTRY & MATERIALS SCIENCE**

   By simulating complex chemical reactions and interactions that are difficult or impossible to model with classical computers, quantum computing may be able to greatly accelerate the discovery of new materials and drugs.

3. **ADVANCEMENTS IN CRYPTOGRAPHY**

   Quantum computing could potentially break many of the encryption algorithms used to secure sensitive information today. However, researchers are also working on developing new quantum-safe encryption methods that would be resistant to attacks by quantum computers.

4. **OPTIMIZATION & MACHINE LEARNING**

   Quantum computing could be used to solve optimization problems that are intractable for classical computers, such as those encountered in logistics and supply chain management. Quantum machine learning could also offer significant improvements in data analysis and pattern recognition.

5. **HYBRID CLASSICAL-QUANTUM COMPUTING**

   Many applications may require a combination of classical and quantum computing to achieve the best results. Researchers are developing methods for integrating classical and quantum algorithms to take advantage of the strengths of each approach.

   Overall, the future of quantum computing is bright, with the potential to revolutionize fields ranging from medicine to finance to cybersecurity. Even so, quantum computing may not be widely accessible and practical for real-world applications for several years.

7 Quantum Computing Companies of The Future

We will now take a look at some of those newer startups and companies in the space, founded within the last year or two, that are innovative in their approaches and have a good chance to unlock some of the possibilities of quantum technology.

- ABELIAN
- PLANQC
- BOHR QUANTUM TECHNOLOGY
- DIRAQ
- SCALINQ
- SANDBOXAQ
- BLUEQUBIT

How Bright Is The Future of Quantum Computing

As quantum computing advances, a world that is currently science fiction will become a reality. With it, we will be able to process enormous amounts of data extremely fast, enabling simulations that are unimaginable at the moment. As a result, a whole new level of AI will be possible that will accelerate ad-

vances in genomics, disease management and renewable energy technologies, just to name a few. In a world in which the cost of energy is rapidly falling toward zero, we will live longer, healthier lives.

Let us hope, however, that when the technology becomes more powerful and more mainstream, we use it for only good intentions.

24.Scientists Are One Step Closer to Quantum Internet

by News Staff
https://www.sci.news/physics/quantum-internet-diamond-nanostructures-11811.html

“Diamond material is of great importance for future technologies such as the quantum internet,” said senior author Professor Tim Schröder from the Humboldt-Universität zu Berlin and his colleagues.

“Special defect centers can be used as qubits and emit single light particles that are referred to as single photons.”

“To enable data transmission with feasible communication rates over long distances in a quantum network, all photons must be collected in optical fibers and transmitted without being lost.”

“It must also be ensured that these photons all have the same color, i.e., the same frequency.”

“Fulfilling these requirements has been impossible — until now.”

In their research, the authors were able to generate and detect photons with stable photon frequencies emitted from quantum light sources, or, more precisely, from nitrogen-vacancy defect centers in diamond nanostructures.

“This was enabled by carefully choosing the diamond material, sophisticated nanofabrication methods, and specific experimental control protocols,” they said.

“By combining these methods, the noise of the electrons, which previously disturbed data transmission, can be significantly reduced, and the photons are emitted at a stable (communication) frequency.”

The team’s results show that current communication rates between spatially separated quantum systems can prospectively be increased more than 1,000-fold — an important step closer to a quantum internet.

“We integrated individual qubits into optimized diamond nanostructures,” they said.

“These structures are 1,000 times thinner than a human hair and make it possible to transfer emitted photons in a directed manner into glass fibers.”

“However, during the fabrication of the nanostructures, the material surface is damaged at the atomic level, and free electrons create uncontrollable noise for the generated light particles.”

“Noise, comparable to an unstable radio frequency, causes fluctuations in the photon frequency, preventing successful quantum operations such as entanglement.”

"A special feature of the diamond material used is its relatively high density of nitrogen impurity atoms in the crystal lattice."

"These possibly shield the quantum light source from electron noise at the surface of the nanostructure."

"However, the exact physical processes need to be studied in more detail in the future," said first author Dr. Laura Orphal-Kobin, also from the Humboldt-Universität zu Berlin.

The research is published in the journal *Physical Review X*.

25.The Journey Towards Post-Quantum Cryptography

by Dashveenjit Kaur
https://techwireasia.com/2023/04/why-is-there-so-much-hype-on-post-quantum-cryptography/

Post-quantum cryptography refers to cryptographic algorithms and protocols designed to be secure against attacks by quantum computers. According to McKinsey, while quantum computers may not be able to crack conventional encryption protocols until 2030, many cybersecurity and risk managers should evaluate their options now.

For starters, quantum computing holds promise for problems out of reach for currently available high-performance computers. However, the technology's power poses a significant cybersecurity risk because quantum computers can break many cryptographic algorithms presently used to secure our digital communications.

That said, the purpose of post-quantum cryptography in today's day and age is to ensure that digital communications and data remain secure against potential attacks from quantum computers. Quantum computers can break many of the cryptographic algorithms currently used to secure our digital systems, such as online transactions, banking systems, and communication networks.

Key elements involved in post-quantum cryptography

Cryptographic security is achieved by using mathematical problems that are believed to be challenging even for quantum computers to solve, such as lattice-based cryptography, code-based cryptography, and hash-based cryptography. Post-quantum cryptography will also become the standard for cryptographic protocols in the coming years.

It is important to note that transitioning to post-quantum cryptography is a complex process that requires careful planning and coordination, as it involves updating the entire cryptographic infrastructure of our digital systems. According to the National Institute for Standards and Technology (NIST), large quantum computers will be powerful enough to breach vital public schemes currently in use in a few years.

In 2022, US President Joe Biden signed the Quantum Computing Cybersecurity Preparedness Act to prepare for such incidents. By July 5, 2023, the Office of Management and Budget show will begin implementing the NIST-approved cryptographic algorithm to protect systems in the executive branch. Microsoft, AWS, VMWare, Cisco Systems and Samsung are among 12 companies the NIST has selected to guide the nation's migration to cryptographic standards that are immune to the computation powers of a

quantum machine.

At the same time, the Cybersecurity and Infrastructure Security Agency (CISA) also established a Post-Quantum Cryptography (PQC) Initiative to unify and drive agency efforts to address threats posed by quantum computing. In coordination with interagency and industry partners, CISA's new initiative is building on existing Department of Homeland Security (DHS) efforts as well as those underway at NIST to support critical infrastructure and government network owners and operators during the transition to post-quantum cryptography.

CISA's PQC Initiative will oversee its activities in four critical areas:

- **Risk Assessment**: Assess vulnerability across the U.S. critical infrastructure by assessing risk in the 55 National Critical Functions (NCFs). Through this macro-level assessment of priority NCFs, CISA will determine where post-quantum cryptography transition work is underway, where the greatest risk resides, and what may require federal support.

- **Planning**: Plan where CISA and its partners should focus resources and engagement with owners and operators across public and private sectors.

- **Policy and Standards**: Work with partners to foster adoption and implementation of policies, standards, and requirements to improve the security of the Federal Civilian Executive Branch (FCEB), state, local, tribal, and territorial (SLTT) entities; critical infrastructure; and the underlying technology that supports all of these entities.

- **Engagement and Awareness**: Engage stakeholders to develop mitigation plans and encourage implementation of standards once they are available across the FCEB, SLTT, and critical infrastructure sectors. Develop technical products to support these efforts.

It is also important to note that implementing post-quantum cryptography requires updating the entire cryptographic infrastructure of digital systems, including software, hardware, and communication protocols. This may take several years to complete and will require careful planning and coordination.

Some general steps to be considered in implementing post-quantum cryptography include evaluating current cryptographic infrastructure, which involves assessing current cryptographic protocols, algorithms, and keys to identify areas that need to be updated to provide post-quantum security.

That step is followed by selecting post-quantum cryptographic algorithms that meet security requirements and are compatible with an organizations' systems. Once that is done, businesses should perform extensive testing and validation of the post-quantum cryptographic algorithms to ensure they are secure and work correctly.

Last but not least, communicate the changes to all relevant parties, including customers, employees, and partners, to ensure that they know the new post-quantum cryptographic protocols and can adjust their systems accordingly.

26.SK Telecom Touts Telecom Network Quantum Cryptography Integration

by Dan Meyer

https://www.sdxcentral.com/articles/news/sk-telecom-touts-telecom-network-quantum-cryptography-integration/2023/04/

SK Telecom said it has developed technology that allows for integrated management of quantum cryptography network equipment from different vendors using SDN and distributing quantum keys in an automated manner. The move could be an important step toward integrating quantum cryptography network equipment into next-generation telecommunication networks.

The SK Telecom technology, which it's clearly labeling as "quantum cryptography communication networks of diverse manufacturers," has completed verification testing at the Korea Advanced Research Network. The South Korea-based telecom operator is also attempting to promote the technology for acceptance into the European Telecommunications Standards Institute (ETSI) global standards bodies.

That work is around a "control interface of software-defined networks" and an "orchestration interface of software-defined networks for interoperable key management system."

The first is to provide an abstraction layer that allows an operator to use a common SDN protocol to control the flow of information across a quantum signal or a traditional signal medium. The second provides an orchestration layer for management of quantum encrypted communications across both a full quantum channel and a separate optical transport network channel.

SK Telecom noted ETSI accepted those tasks last month as work items for its quantum key distribution (QKD) industry specification group.

"The two standardization tasks approved as work items by ETSI will boost the expansion of quantum cryptography communication in the global market," Ha Min-yong, chief development officer at SK Telecom, noted in a statement. "We will work with diverse global players in many different areas to create new business opportunities in the global market."

Quantum for telecom

Quantum cryptography communication transmits each bit of information as a single photon of light, which encrypts that information against eavesdropping or decryption. Telecom operators and vendors have been working for several years on integrating that level of encryption into networks.

For instance, Toshiba and the Tohoku Medical Megabank Organization at Tohoku University used quantum technology in 2018 to hit one-month-average key distribution speeds exceeding 10 Mb/s over installed optical fiber lines. They also used the technology to monitor the performance of installed optical fiber lines in different environments.

Toshiba later partnered with U.K.-based operator BT on using QKD across to secure a network transmission.

SK Telecom also has a long quantum history, including work with Swiss-based strategic partner ID Quantique, which focuses on quantum cryptography communication technology.

Industry trade group GSMA last year announced its Post-Quantum Telco Network Taskforce focused on supporting the industry's creation of a roadmap to secure networks, devices and systems across the entire supply chain." That work was initiated with IBM and Vodafone, and has since gained more than 45 members.

Lory Thorpe, GSMA Post-Quantum Telco Networks chairperson and head of IBM Consulting's Telco Transformation Offerings, told SDxCentral last month that the core objective of the taskforce is to ensure

the implementation of the right requirements and standards in a timely manner to avoid being “late to the party.” Thorpe explained the initial problem statement was “around how do we support the telco ecosystem to navigate the path to quantum safe.”

“When you look at where cryptography is used in telco systems, it impacts basically all of the different systems. But it also then impacts all of the standards that underpin these systems as well,” she said. “We’re advocating that people start planning, not panicking, but at least planning because … this isn’t something that just happens overnight.”

27.Mitigating Side-Channel Attacks in Post Quantum Cryptography (PQC) with Secure-IC Solutions

https://www.design-reuse.com/industryexpertblogs/53785/mitigating-side-channel-attacks-in-post-quantum-cryptography-pqc.html

Interview with Khaled Karray, our expert on side-channel attacks

Side-channel attacks (SCA) form an often-overlooked security vulnerability for electronic systems. However, if you want to ensure a comprehensive security, SCA protection should be part of the mix. Khaled Karray explains how Secure-IC’s IP blocks help you keep safe.

Khaled Karray is our senior expert in embedded system security and side-channel attacks. After graduating in Computer Science and Telecommunications Engineering from the Tunisia Polytechnic School, he obtained a master’s degree from the University of Montpellier (France) in Microelectronics. He then enrolled in a PhD program with PSA Group (Stellantis since 2021) at the University of Paris-Saclay (Télécom ParisTech).

He has held several positions at Secure-IC as program manager for pre-silicon security evaluation tools as well as System Level Automotive security. Khaled currently leads the Threat Analysis Business Line in charge of the development of advanced tools for evaluating hardware and software security of embedded systems.

At Secure-IC, he follows the latest in SCA protection and advises on how to best secure the implementations of security algorithm in the IP blocks. He also keeps an eye on new and future developments. That way, our blocks are future proof and our specialists are already preparing for next generations of SCA threats.

KHALED, FIRST THING FIRST: WHAT ARE SIDE-CHANNEL ATTACK AND WHY SHOULD PEOPLE CARE?

A SCA is a way of breaking into a computer system by exploiting physical signals that the system leaks. This is the equivalent of trying to break into a strongbox by listening to the click sounds that the mechanical lock makes in various positions.

Instead of exploiting logical weaknesses in the algorithms or implementations – the classical way of hacking – the attackers will monitor for example the variation in power consumption of a system, the

electromagnetic radiation it emits, or the time it needs to execute certain cryptographic tasks. In fact, they may exploit any source of information that is not a standard input/output signal.

A SIDE-CHANNEL ATTACK IS BASED ON INFORMATION COLLECTED FROM OBSERVING THE OPERATION OF THE SYSTEM OVER A PERIOD, RATHER THAN SOME WEAKNESSES IN THE IMPLEMENTED SECURITY ALGORITHM.

With that information, they may work out information about a system: the algorithms it uses, the security measures that are applied, or even the cryptographic keys.

Simple SCAs require some technical knowledge of the internal operation of a system. However, there are also sophisticated methods that use statistical analysis of signals and that can be used as general, blackbox attacks.

HOW DO HACKERS GET ACCESS TO THE HARDWARE? YOU'D THINK THAT TODAY'S DATA CENTERS ARE ADEQUATELY PROTECTED, ALSO PHYSICALLY?

Yes, they are. There is another issue though, a huge opportunity for hackers. Networked edge devices are everywhere now, think of processors in automotive electronics, medical devices, or smart manufacturing machinery. There are now hundreds of millions of devices out there that are physically accessible to hackers. Devices that they can prob and test as much as they want. Devices that are not always so well protected and through which they could get further access to the core of an application.

Not only today's many edge devices are vulnerable to SCAs. More complex SoCs that contain a processor and a ASIC/FPGA within the same die may also become a target. These complex SoCs often have a secured and unsecured area, which amongst others contains analog-to-digital converters that can perform power measurements. Assuming an attacker rst gained the ability to run code on the unsecure side of a device, they could then use the on-board analog-to-digital converters to capture power traces of the hardware encryption engine. That way, an advanced SCA could be staged to retrieve the secret keys.
.
.
.

28.Eviden to Launch First 'Post-Quantum Ready' Solutions for Digital Identity

by Atos International
https://www.globenewswire.com/news-release/2023/04/05/2641634/0/en/Eviden-to-launch-first-post-quantum-ready-solutions-for-Digital-Identity.html

Eviden, the Atos business leading in digital, cloud, big data and security today announces the evolution of its digital identity management products so that they will be ready for the post-quantum era by the end of the year.

While powerful quantum computers will be able to break classical cryptography within a few years, post-quantum cryptography[4] (PQC) represents the most promising avenue to thwart the quantum threat. As

[4] Post-Quantum Cryptography (PQC) is a family of cryptographic algorithms including key establishment and digital signatures that ensures a conjectured security even against an attacker equipped with quantum computers.

technology is making progress, new cryptographic algorithms and methodologies are being specified and developed in cooperation between the scientific community, standardization bodies and industry.

Eviden's product evolution will allow customers to anticipate the coming revolution, planning the migration of their cybersecurity solutions to gradually increase trust in post-quantum algorithms, with complete peace of mind.

The Eviden cybersecurity products for Digital Identity that will be 'post-quantum ready' soon are:

- **IDnomic PKI** – a powerful, multi-purpose Public Key Infrastructure software suite for production and issuance of trusted digital identities, compliant to highest security standards. Crypto-agile *by design*, IDnomic PKI will guarantee a smooth migration path for customers by issuing hybrid certificates for legacy and 'post-quantum cryptography ready' applications.

- **Cryptovision GreenShield** – a solution for email and file encryption, approved for the exchange of classified information (EU and NATO restricted, EUCI, VS-NfD certified), accredited by the German BSI and approved by the European Council. Its architecture is modular and flexible, based on crypto-agile development. PQC readiness will enable seamless use of traditional algorithms, as well as future quantum-resistant ones.

"With the soon coming quantum revolution, now is not the time for panic, but for planning! With its leadership in cybersecurity and pioneering approach to science and technology, Eviden has extensive expertise in post-quantum cryptography. We are delighted to announce that customers will benefit from a new version of our state-of-the-art digital identity products, ready to kick-start this exciting post-quantum cryptography revolution with future-proof solutions." said **Jean-Philippe Poirault, CEO Big Data and Security, Eviden, Atos Group.**

IDnomic PKI and Cryptovision Greenshield 'post-quantum cryptography ready' will be available by Q4 2023.

Post-quantum cryptography is at the core of Eviden's work, as Eviden also supports post-quantum algorithms with its Trustway Proteccio HSM. In addition, the Atos Group, through its Eviden business line, is a pioneer in quantum computing. The Group launched the first quantum emulator on the market in 2016 and now offers the most powerful quantum computing application development platform, coupled with a consultancy offering that accelerates real quantum applications through all-in-one capabilities and a best-in-class development environment.

29.On-Chip (FPGA, MCU, SoC) Generation of Post-Quantum Secure IDs and Keys

by Max Maxfield
https://www.eejournal.com/article/yes-on-chip-fpga-mcu-soc-generation-of-post-quantum-secure-ids-and-keys/

Just to keep things interesting, we're going to come at things from a slightly different direction to my usual columns. First, I'm going to tell you something you already know. Second, I'm going to tell you something of which you are probably aware. Third, once I've lulled you into a false sense of security, I'm going to surprise you with something new (be afraid, be very afraid).

Something You Already Know

Let's start with the fact that there are a lot of "things" hanging of the end of the internet of things (IoT) at the edge where sensors and actuators and suchlike interface with the real world (assuming we aren't all part of a Matrix-like simulation, in which case all bets are off and I'll just keep on taking the pills, although I no longer recall which color is best).

How many things are we talking about? I no longer have a clue. One number that's often bandied around is 50 billion devices by 2030. Meanwhile, Statista offers a slightly more modest prediction of 30 billion devices by 2030. Whichever of these numbers is closest to the mark, that's a lot of devices, however you look at it.

The problem from a security point of view is that, unless protected, each of these devices offers a potential attack vector for ne'er-do-well hackers and nefarious nations. As reported in *Forbes*, a classic case we all recall from 2017 is when hackers compromised an IoT device used to remotely monitor and adjust the temperature and salinity in a fish tank that had recently been installed in a Casino. Via this device, the hackers gained access to the Casino's network and managed to exfiltrate 10 gigabytes of data, including juicy tidbits of information on high-roller gamblers.

That was six years ago. A lot has changed since then, including the fact that our persons and our homes are becoming increasingly connected with things like wearable health monitors, camera-equipped voice assistants, Ring doorbells, video baby monitors, and Roomba floor-cleaning robots equipped with cameras that they use to help them create a floorplan. It's not beyond the bounds of possibility that future high-tech burglars could compromise one or more of these devices and use the information thus gathered to decide who to steal from next.

As an aside, did you see my recent Cool Beans Blog *Do Furbys + ChatGPT = AI Apocalypse?* This torrid tale involves a programmer who augmented a Furby with speech recognition capabilities, hooked it up to ChatGPT, and posted the question: "Was there a secret plot from Furbies to take over the world?" The response from that cute little Furby's mouth may well send shivers up and down your spine.

Something of Which You Are Probably Aware

One "brick" in the foundation of a secure system is to be able to uniquely identify each and every device that has any sort of "intelligence" in the form of processing capabilities. This includes microprocessor units (MPUs), microcontroller units (MCUs), graphic processing units (GPUs), neural processing units (NPUs), field-programmable gate arrays (FPGAs), and system-on-chip (SoC) devices, to name but a few.

Another "brick" is the cryptographic keys that are used to implement encryption and decryption functions, along with digital signatures and certificates.

One of the problems associated with all of this is how to generate and load any unique identifiers and cryptographic keys into the device. If they start off outside the device, they are vulnerable to being stolen and/or cloned by the very people entrusted with their care. Even if they make it into the system untouched, any IDs and keys that are stored in the device are vulnerable to different forms of attack. What we need is some way for each chip to generate any IDs and keys "on the fly" as required.

All of this leads us to Intrinsic ID. Founded in 2008, Intrinsic ID has built an enviable reputation as the world leader in PUF (physical unclonable function, sometimes *physically* unclonable function) technology.

The idea here is that deep sub-micron variations in the production process give slightly random electrical properties to every transistor on a silicon chip. In the case of SRAMs, this randomness is expressed as

the start-up values (0 or 1) in each of the SRAM cells.

These start-up values create a highly random yet repeatable pattern that is unique to each chip. The majority of the cells will power up the same way each time. Of course, some of the cells may power-up in either state depending on their mood of the moment. These cells may be affected by environmental conditions like temperature, and they may change their preferred power-up state over time as the device ages.

The folks at Intrinsic ID have come up with a way of "wrapping" an SRAM PUF with an error-correcting algorithm that results in an unchanging "silicon fingerprint" that can be used to build the foundation of a security subsystem. This PUF technology offers extreme reliability from -55°C to +150°C with a lifetime of 25+ years. As we see in this video, this includes using the PUF as part of a hardware root-of-trust (RoT); that is, a source that can always be trusted within a cryptographic system.

The end result is that devices equipped with Intrinsic ID's IP offer the highest security in the industry. There are no keys "at rest," the technology supports a Zero Trust supply chain, and it works with all foundries and process technologies (it's been implemented in processes from 180nm down to 3nm) in standard silicon with no extra process steps required.

In many ways, the results speak for themselves. Intrinsic ID has a solid patent portfolio in PUF technology, and its IP already serves multiple markets. In addition to the IoT, Intrinsic ID's technology is found in datacenters and high-performance computing (HPC) facilities, in aerospace and defense, and in any application that demands secure transactions.

With 100+ design wins, 10+ global certification and government program wins, and four out of the top five MCU vendors as customers, Intrinsic ID's IP can boast more than 500+ million deployments in the field.

Wait! What? Why so few?

On the one hand, 500+ million deployments are nothing to be sniffed at (we should all be so lucky as to create something so prolific). On the other hand, 500+ million is but a drop in the bucket when we consider how many IoT devices are already roaming the world, and how many we expect to join them in the not-so-distant future.

So, what's the problem? Well, as wonderful as Intrinsic ID's technology is, thus far it's been realized in the form of hardware IP. This has meant that the creators of MCUs, FPGAs, SoCs, etc. have had to instantiate the PUF as an additional block of IP. Also, that all the processing (key generation, etc.) has been implemented in hardware. This has proved to be a fly in the soup or an elephant in the room for a lot of players (I never metaphor I didn't like).

Something New to Surprise You

I feel a bit like the proverbial "iron hand in a velvet glove"; first I brag on the wonders of Intrinsic ID's technology, and then I pull the rug out from under my own feet. But wait, there's more, because "I come to praise the folks at Intrinsic ID, not to bury them" (with apologies to the Bard of Avon).

I was just chatting to Pim Tuyls, who is the Founder of, and CEO at, Intrinsic ID. As part of our conversation, Pim explained how Intrinsic ID unveiled something new at the recent Embedded World Conference and Exhibition, which was held 14-16 March 2023.

Pim started by noting that billions of devices need an unclonable identity, trillions of cryptographic keys need to be stored securely, and trillions of connections between connected devices need to be authenti-

cated. The trick, of course, is coming up with a solution to establish and scale robust security.

This is the point where we can all break out our party hats, because such a solution has arrived in the form of Intrinsic ID's new Zign X00 series of software products, which can be deployed in every digital device that offers processing capabilities (MCUs, FPGAs, SoCs, etc.) under the sun. This includes devices that have already been built and systems that have already been deployed.

The idea here is that every digital device that offers processing capabilities already has some amount of SRAM. All that is required is to set a small amount (1KB) of this SRAM aside to be used as the device's PUF. All of the other functions are realized in software code rather than hardware logic gates.

The software is created in C that will run on any CPU—it doesn't matter if the CPU is Arm, ARC, MIPS, RISC-V, X86, Xtensa, or whatever. Whichever CPU you are using, the software (leveraging the SRAM PUF) will provide you with all the security features you need, from random number generation, key generation, key management, encrypting other secrets on the device, encrypting and decrypting communications, authentication, and full public key cryptographic activities like setting up shared keys and creating signatures.

This software is delivered in the form of a compiled library (along with API specifications and a user manual) targeted at the CPU of your choice. Your application makes API calls into this library to access the required functions. If you wish to use existing hardware accelerators on your device for tasks like encryption and decryption, then the software includes interfaces that let you configure and connect to said accelerators.

There are currently three members in the Zign X00 Series: the Zign 100, 200, and 300, with Flash memory footprints ranging from 7KB to 30KB, depending on the member and options selected.

The **Zign 100** API enables IoT developers to generate unique device identities, secure cryptographic keys, and random values. It enables easy and collision-free identification of billions of devices from various vendors. Zign 100 can also be integrated as a hardware-based trust anchor for Mbed TLS, OpenSSL, wolfSSL, and other libraries, extending the chain of trust beyond just a single device.

The **Zign 200** is a secure key generation, management, and storage solution for any IoT device. Zign 200 offers functions to wrap and manage secret keys and encrypt data, which can then be stored in unprotected memory or can be securely transmitted over the network. Zign 200 also offers random values, generated by a NIST 800-90A/B-compliant random number generator and a collision-free unique device identity.

The **Zign 300** is the Crème de la crème. To solve security problems in IoT systems, such as authentication, product lifecycle management, reverse engineering and cloning, every device needs an unclonable identity. This consists of a secret key, a public key and a certificate. The biggest challenge is to get these credentials into the device and keep the secret key secret. This can be achieved using Zign 300, which offers the strongest protection of the device secret key and the strongest authentication via unclonable identities. Zign 300 offers all the features of Zign 200. In addition, Zign 300 offers asymmetric cryptography: public key crypto functions such as ECDSA sign and verify, and ECDH shared secret. Public key infrastructure (PKI) elements, such as ECIES and certificate signing request (CSR) are optional.

All of the Zign X00 solutions are post-quantum secure!

Security is a complex topic. It makes my head hurt. I used to enjoy the old days when all we had to do was to create cunning applications that made people gasp "Ooh" and "Aah." I feel sorry for today's developers who must meander their way through the security morass on top of everything else they have to do. I also feel sad for the device manufacturers who have to add additional functions to their components, and for system architects who are prevented from using their desired processing devices due to

the lack of aforementioned security features.

The lads and lasses at Intrinsic ID have addressed all these problems in a single stroke. They've made it orders of magnitude easier to implement security for the 21st Century (did I mention that these solutions are post-quantum secure?), even with existing processing devices like low-end MCUs and currently deployed SoCs that don't have any security features implemented in hardware.

Personally, I think this is an awesome solution and I believe Intrinsic ID is poised to take the world of security by storm. From 500+ million deployments of their hardware IP today, I expect to see billions of deployments of their software IP in the not-so-distant future. How about you? Do you have any thoughts you'd care to share on this topic?

30.How Post-Quantum Encryption Mandates Affect Healthcare

by Marianne Kolbasuk McGee
https://www.bankinfosecurity.com/interviews/how-post-quantum-encryption-mandates-affect-healthcare-i-5239

A 3-month-old federal law meant to future-proof federal computers from quantum computer decryption will have an effect on healthcare sector entities, too, says Mac McMillan, founder and CEO emeritus of privacy and security consulting firm CynergisTek.

"Data and systems that we have today that use at least the current cryptography standard will no longer be adequate when quantum computing becomes mainstream," he said (see: *Biden Signs Law to Safeguard IT Against Quantum Computing*).

Ultimately, private sector organizations, including healthcare entities - "whether they like it or not" - also will need to migrate to the new cryptographic standards, which are being hammered out by the National Institute of Standards and Technology, the National Security Agency and others, according to McMillan.

The eventual mass migration to post-quantum cryptography will compel healthcare entities to take "a 100% inventory" of their network ecosystems, he said. "Everywhere you have encryption, you will need to consider upgrading to the new standard in order to protect that data."

"Right now, if I were a CISO at a health system, I would be looking at this legislation and say, 'Even though I'm not a federal agency and it doesn't apply to me directly, I'm going to start working with IT to identity the systems, applications and data that we need to be thinking about for migration and putting together a plan so that by the time the new standards come out, we're prepared to do that."

In the interview, McMillan also discusses:

- The types of healthcare sector organizations most likely at risk for potential quantum computing attacks;
- The threat posed by "harvest now, decrypt later" attacks involving the theft of data currently encrypted using current cryptography standards;
- The systems and devices used in healthcare that potentially present the biggest challenges for

post-quantum cryptography migration.

McMillan is co-founder and CEO emeritus of CynergisTek, which was acquired last year by privacy and security consultancy Clearwater. He has more than 40 years of security and risk management experience, including 20 years at the U.S. Department of Defense and its Defense Threat Reduction Agency.

31.$1M NSF Award Supports Reimagining Cryptography in A Post-Quantum World

by Melissa Brachfeld
https://today.umd.edu/1m-nsf-award-supports-reimagining-cryptography-in-a-post-quantum-world

In 1994, mathematician Peter Shor developed an algorithm showing how then-hypothetical quantum computers could factor numbers exponentially faster than standard machines. This promise of exotic computational power launched the age of quantum computing. It also set the clock ticking on existing public-key cryptography that provides safeguards for online banking, medical records, national secrets and more based on the infeasibility of factoring massive numbers.

Today, with Google, IBM and College Park-based startup IonQ racing to introduce the world's first general-purpose quantum computer, University of Maryland researchers—backed by $1 million in funding from the National Science Foundation—are developing a framework for cryptographic systems that can weather increasingly powerful quantum computers. They are also focused on fundamentally changing the way that cryptography is taught, developed and practiced.

"The aim of our work is to help build the foundational theory of cryptography in a post-quantum future," said Jonathan Katz, a professor of computer science and principal investigator of the award. "We know that many aspects of classical cryptography will look very different in a world where everyone, both honest parties and attackers, have access to quantum computers."

Assisting Katz on the NSF award are Dana Dachman-Soled, an associate professor of electrical and computer engineering, and Gorjan Alagic, an associate research scientist in the University of Maryland Institute for Advanced Computer Studies (UMIACS), where Dachman-Soled also holds an appointment.

The researchers will explore constructions of cryptosystems that can be proven secure against quantum computers. Initially they will focus on the private-key setting. Two kinds of cryptography are currently in use: public-key and private-key. The former is ideal for negotiating a connection over the internet but slow for sending data. The latter is very fast but needs a preexisting, already-negotiated connection. In practice, both types get used often.

It is known that quantum computers would pose a dangerous threat to current public-key cryptosystems, Alagic said, but security of private-key systems against quantum computers is less well understood. One strategy is to establish mathematical theorems that say things like, "breaking this private-key cryptosystem would take a quantum computer that's *this* powerful."

Alagic and the other researchers are working closely with the National Institute of Standards and Technology in this area, as the federal agency is ultimately tasked with establishing the benchmarks for any post-quantum security regulations or protocols.

A key element of the NSF grant is to explore new options in education, Katz said. While cryptography in

a post-quantum future will require people to think differently about the challenge of securing critical information, it will also require new knowledge on quantum-based security features that are not currently possible.

Educational initiatives are already underway, with the UMD faculty helping organize a summer school on quantum and post-quantum cryptography at the University of California, Los Angeles last year. The weeklong event brought together physicists and computer scientists and included introductory talks on cryptography and quantum computing, invited talks on post-quantum assumptions and proof techniques, and poster and mentoring sessions.

Dachman-Soled said that although she believes existing public-key cryptosystems will remain in use for the near future, she is incorporating a module on post-quantum cryptography in the undergraduate course she teaches at UMD.

She is also working with a team of Gemstone Honors Program students to extend the functionality of a toolkit she developed to analyze the security of post-quantum cryptosystems when "side-information" is available. Examples include a system's timing, power consumption and electromagnetic leaks, which can be used as a sort of "hint" in attacks to break the cryptosystem, Dachman-Soled explained.To get younger students interested in quantum cryptography, Alagic recently visited an elementary school and a middle school in Montgomery County, Md., as part of each school's career-day programming.

"The kids were great," he said. "The elementary school students enjoyed it so much they actually sent me thank-you notes encrypted with the Caesar cipher I taught them."

32.The Impact of Quantum Computing on Cybersecurity

by Dilki Rathnayake
https://www.tripwire.com/state-of-security/impact-quantum-computing-cybersecurity

Quantum computers can solve highly complex problems faster than any of its predecessors. We are currently in a period of a quantum revolution. Many organizations are currently investing in the quantum computer industry, and it is predicted that the quantum computing market may increase by 500% by 2028.

Due to their powerful computing capabilities, the Cloud Security Alliance (CSA) has estimated that by April 2030, RSA, Diffie-Hellman (DH), and Elliptic-Curve Cryptography (ECC) algorithms will become vulnerable to quantum attacks. This makes many organizations vulnerable to "harvest now, decrypt later" (HNDL) attacks, where attackers harvest data from organizations to decrypt when quantum computing reaches its maturity and the cryptographic algorithms become obsolete. In a new Deloitte Poll, 50.2% of the respondents believe that their organizations are at risk for HNDL attacks.

The quantum threat towards cryptography

In quantum computing, the basic unit is qubits (quantum bits), but, more than the classical computing bits which exist in 0 or 1 states, qubits can exist in 0, 1, or in both combinations. Through manipulation of the information in the qubits, high-quality solutions can be provided for difficult problems. The IBM report on security in the quantum computing era states that all Public Key Cryptography (PKC) standards could become vulnerable in the next few years. The exposure of sensitive data will most likely es-

calate to other risk scenarios, and this will affect communication networks, electronic transaction verifications, and the security of digital evidence as well.

Quantum-resistant or quantum-safe cryptography standards are currently being implemented and the National Institute of Standards and Technology (NIST) has already chosen the first group of encryption tools that would withstand quantum attacks. This was the result its six-year-long competition. They have also initiated a Post-Quantum Cryptography Standardization project to produce quantum-resistant algorithms.

Quantum Key Distribution (QKD)

Quantum Cryptography, more accurately described as Quantum Key Distribution (QKD), is a quantum-safe method introduced to exchange key exchange between two entities. It works by transmitting photons, which are polarized light particles, over a fiber optic cable. QKD protocols are designed according to the principles of quantum physics. Hence, observation or eavesdropping on a quantum state causes perturbation because the unique and fragile properties of photons prevent passive interception. This perturbation will lead to transmission errors. This will be detected by the endpoints, and the key will be discarded. This is used as a verification of the distributed keys. Currently, QKD is just limited to distances of less than 100 kilometers, but satellite proof-of-concept suggests that it can be expanded to more distances over the next few years.

The quantum future

There is an ongoing quantum revolution that will transform entire computer processes, enhancing the security and privacy of communications. However, this may also introduce many new cybersecurity threats. According to the Deloitte poll, organizations are preparing for quantum computing cybersecurity risks. 45% of the respondents are almost complete with their assessments of post-quantum encryption vulnerabilities, and only 11.7% are reported to be taking a “wait and see” approach for a cyber incident to take place.

There are many Quantum-as-a-Service (QaaS) providers that offer quantum services for researchers, scientists, and developers. Since threat actors might target the QaaS providers and their users, these providers should deploy stringent security protocols in order to access the services. The emerging field of quantum machine-learning could also produce more effective algorithms for identifying and detecting new cyber-attack methods.

The following practices can help your organization prepare for quantum computing cybersecurity:

- Engaging with standard organizations – Organizations such as NIST, and CISA, provide updates of new standards.
- Inventory critical data – Crucial for future analysis to plan which data would be most at risk in a post-quantum environment.
- Inventory cryptographic technologies in your environment – Knowing which technologies use cryptographic functions will enable your organization to address potential risks and impacts.

Many are curious about the revolution of quantum computing and its post-quantum effects. Currently, researchers and scientists are still carefully studying the topic. It is always best to approach the quantum threat as much as any other vulnerability, and prepare for quantum-safe protection.

