Crypto News

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

September 01, 2023

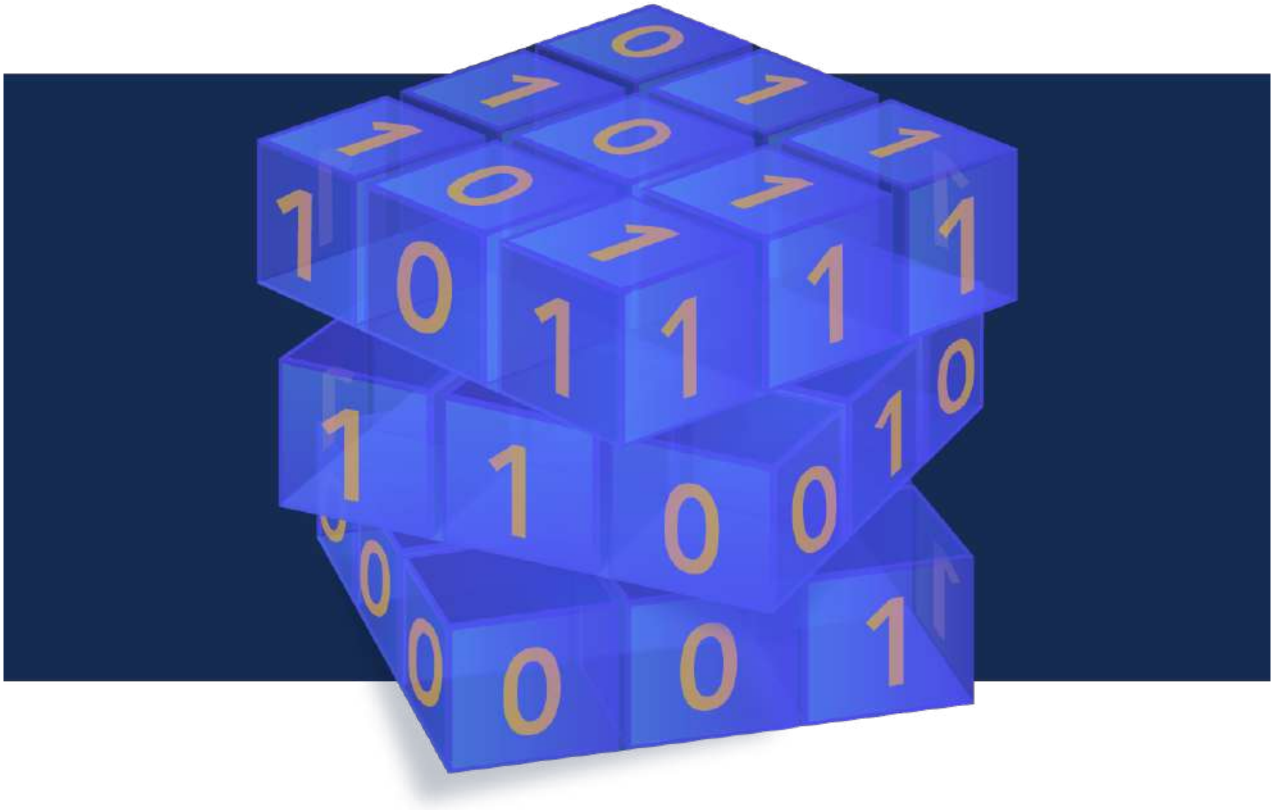


TABLE OF CONTENTS

Editorial

I bet there are some things you've heard about quantum computers that had you asking whether they're true or not. Perhaps it's about whether quantum computers will one day replace all classical computers. Maybe you're thinking about the financial aspects and due to the expensive price tag of quantum computers you conclude that logically only governments and big businesses will be able to use them. Perhaps your doubts are more around the practical use cases for quantum computers. The author of article 16 would like to provide their insight and debunk the top 5 quantum computing myths in the industry including those listed above. From quantum computing experts to quantum computing enthusiasts and everyone in between, this article is a good read that will lead to rousing discussions that I'm more than looking forward to having with my colleagues and friends.

In other exciting news, for those following NISTs journey with quantum computing and post-quantum cryptography (PQC), the wait is over. NIST released their first draft of the standards for PQC a few weeks ago which are now open for public comment. This comes after they selected four algorithms last year of which three now have these draft standards. For those who have been keeping an eye on PQC as a solution for to the weaknesses of RSA and ECC with Shor's algorithm running on a quantum computer, this is yet another large step forward toward a more secure future. But of course, there is still a need for the submission of more signature algorithms. Variety surely is the spice of life, and it's also good for finding solid solutions in this case. If you're interested in learning more, make your way down to article 10.

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.SSL Deprecation: Understanding the Evolution of Security Protocols

by Nick France
https://www.sectigo.com/resource-library/ssl-deprecation-understanding-the-evolution-of-security-protocols

Secure Sockets Layer (SSL) is a security protocol that enables encrypted digital communications—between a web browser like Google Chrome or Mozilla Firefox and a web server, for example. SSL certificates authenticate the identity of an online entity and secure online communications with that entity.

SSL was created in 1995, and 2.0 was the first version of SSL used in production. After the introduction of SSL 3.0, standards bodies replaced SSL with Transport Layer Security (TLS), a more secure protocol. However, the term SSL was used so commonly that it persisted as the de facto name for TLS.

When was SSL deprecated?

The Internet Engineering Task Force (IETF) officially deprecated SSL 3.0 in June 2015. While the IETF discouraged the use of deprecated SSL protocols, providers of individual software systems are responsible for determining the SSL 3.0 end-of-life date.

Most organizations have transitioned to the TLS protocol. TLS 1.0 and TLS 1.1 were the older versions, and companies should upgrade to TLS 1.2 and TLS 1.3 whenever possible.

Why SSL was deprecated

In September 2014, a team of Google security researchers discovered a serious SSL 3.0 vulnerability called POODLE, or Padding Oracle on Downgraded Legacy Encryption, which hackers can exploit to decrypt secure communications and steal confidential information. The news diminished SSL's credibility as a reliable encryption method, and security experts recommended SSL be retired.

Additionally, the SSL protocol relied on older encryption algorithms and was no longer enough to protect against new attack techniques. The need for more robust security in the face of evolving cyber threats has led to the TLS protocol.

TLS vs. SSL security protocols

TLS was introduced as SSL's successor and has become the primary cryptographic protocol for the internet. It fixed various SSL security issues, including cipher suite vulnerabilities, POODLE attacks, cipher block chaining (CBC), and renegotiation vulnerabilities.

TLS 1.3, the latest TLS version, is faster and more secure. It uses ephemeral key exchange to reduce the risk of compromised session keys. It also eliminates older cryptographic algorithms for better performance. However, TLS 1.2 is still widely used due to the absence of known vulnerabilities and TLS 1.3's backward-compatibility challenges.

Why do people still refer to TLS as SSL?

SSL's prominence in the early internet days and widespread usage have made it synonymous with secure communication, even long after TLS has taken over. Meanwhile, people who don't have an in-depth understanding of cybersecurity often use the two terms interchangeably, adding to the misconception and confusion.

Today, the term "SSL certificate" is still widely used, even by those in the security industry. For example, many Certificate Authorities (CAs) continue to use "SSL certificate" as a colloquial term for all digital certificates for encryption and authentication. TLS certificates are often called SSL/TLS certificates to simplify communication and avoid misunderstanding.

The future of internet security: Beyond TLS 1.3

We must invest in ongoing efforts to enhance internet security protocols and adapt to emerging threats. TLS will evolve to address vulnerabilities, improve encryption algorithms, and optimize handshakes for faster connections. In particular, quantum computers can easily break traditional cryptographic algorithms, and we expect the TLS protocol to include updates on post-quantum cryptography and quantum-resistant algorithms.

Meanwhile, the validity of TLS certificates is shortening. The 90-day lifecycle will improve the security of online communications. But it will also make it more challenging for organizations to manage their digital certificates effectively to avoid outages and disruptions.

SSL deprecation was a crucial move toward improved online communication security. The TLS protocol addressed critical vulnerabilities and set the stage for future improvement as we head into the quantum computing era. Obtaining TLS certificates from a reputable CA and effective certificate management are critical to ensuring compliance, security, and business continuity.

2.PolarFire FPGAs verified for single-chip cryptography design flow

by Jean-Pierre Joosting
https://www.eenewseurope.com/en/polarfire-fpgas-verified-for-single-chip-cryptography-design-flow/

The UK National Cyber Security Centre (NCSC) has reviewed Microchip Technology’s PolarFire® FPGAs when used with the Single-Chip Crypto Design Flow against stringent device-level resiliency requirements.

System architects and designers now have further evidence of the security of their communications, industrial, aerospace, defense, nuclear and other systems relying on PolarFire FPGAs.

“The NCSC conducts a very rigorous analysis, and the work done with Microchip on the Design Separation Methodology in the PolarFire FPGA enables the user to take advantage of improved resilience and functional isolation within the device. This reinforces Microchip’s commitment to our comprehensive approach to security,” said Tim Morin, technical fellow at Microchip’s FPGA business unit. “This analysis provides the option for single-chip cryptography in addition to what already exists within the devices for protecting IP, securing data and protection against physical tampering—an often overlooked and very powerful threat to every electronic system, especially those at the intelligent edge.”

PolarFire FPGAs implement Microchip’s industry-leading security architecture to protect intellectual property, secure data and secure supply chains.

PolarFire FPGA IP protection includes:

- AES 256-encrypted configuration files with SHA 256-based HMAC authentication.
- Processing is protected against Differential Power Analysis (DPA) with technology licensed from Cryptography Research Incorporated (CRI).
- Public key cryptographic cores: Elliptic Curve Cryptography (ECC) for secure distribution of keys.
- True random number generators.

PolarFire FPGA data security features include:

- Hardened cryptographic accelerators for use in the end application
- Pass-through CRI license enables royalty-free development of DPA-protected algorithms using techniques patented by CRI

PolarFire FPGA supply chain security features reduce the risk of counterfeiting, re-marking and over-building and include:

- Silicon biometrics, including Physically Unclonable Functions (PUFs), that allow each device to be uniquely identified and cryptographically validated

PolarFire FPGAs lead their product category in delivering twice the power efficiency, military-grade security and the industry's highest reliability, which the company will extend with the PolarFire 2 FPGA roadmap as Microchip continues to increase compute capability in ever-smaller and less costly industrial, IoT and other edge-compute products. With their real-time, Linux®-capable RISC-V-based microprocessor subsystem, PolarFire SoC devices are the only SoCs on the market that create new configurable processing capabilities through hardened RISC-V core complexes in a fast FPGA fabric.

The devices are supported by Microchip's Libero® SoC Design Suite available to license, including no-charge versions, from the purchasing and client services website at www.microchipdirect.com. PolarFire FPGA and SoC development kits and hardware are also available

3.SK Telecom seeks standards for quantum-safe communication

by Juan Pedro Tomás

https://www.rcrwireless.com/20230830/security/sk-telecom-seeks-standards-quantum-safe-communications

SK Telecom noted it will be leading efforts to develop standards for key management of hybrid approaches with quantum key distribution (QKD) and post-quantum cryptography (PQC)

Korean operator SK Telecom said it will promote the development of standards for quantum-safe communications at the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Study Group 17 (SG17) meeting, which is being held at the Korea International Exhibition Center

(KINTEX), starting this week through September 8.

ITU-T SG 17 is a statutory group of the ITU-T concerned with security, which holds meetings twice a year to develop international standards and technical reports.

At the meeting, SK Telecom says it will be leading efforts to develop standards for key management of “hybrid approaches” with quantum key distribution (QKD) and post-quantum cryptography (PQC), with the aim of reaching quantum-safe communications by combining the strength of QKD and PQC.

The Asian carrier explained that quantum-safe communication refers to the use of technologies that are resistant to attacks by quantum computers, in order to keep information assets secure even after a large-scale quantum computer has been built.

SK Telecom said it is also actively working to develop and commercialize quantum cryptography technologies. Together with SK Broadband and ID Quantique, SK Telecom says it is not only setting standards for the operation of quantum cryptography communication network built with equipment from different manufacturers at the European Telecommunications Standards Institute (ETSI), but that it has also successfully verified the related technology on the national test network.

“We are excited to lead the establishment of standards for next-generation security technologies that utilize the advantages of quantum key distribution and post-quantum cryptography technologies,” said Ha Min-yong, chief development officer of SK Telecom. “We will continue to make efforts to contribute to the growth of the global quantum cryptography market through active research and business.”

SK Telecom has recently released a 6G white paper that focuses on the key requirements for 6G standardization and the telco’s views regarding the direction of future network evolution.

The Korean carrier said the new white paper contains its views on 6G key requirements and 6G evolution methodology, along with its opinions on the latest trends in frequency standardization. The 6G white paper also provides analysis, development directions and methodologies pertaining to promising 6G use cases, technology trends as well as and candidate frequencies.

Moreover, with the commercialization of 6G, SK Telecom projected that megatrends like AI, power saving and quantum security will spread across all network areas and technologies specialized for each network area—such as radio access network, core network, transport network and aerial network—will be applied and evolved.

4.Expert Marcos Curty: ‘A quantum computer can crack all of our current cryptography’

by Raúl Limón
https://english.elpais.com/science-tech/2023-08-30/expert-marcos-curty-a-quantum-computer-can-crack-all-of-our-current-cryptography.html

Marcos Curty has a doctorate in telecommunications and doesn’t own a cell phone. He says that it is a deliberate and personal choice. Curty aims to transform his hometown, Vigo (northwest Spain), into a global center for security in quantum computing, a significant challenge for this technology. Throughout his international academic career, this professor of signal theory and communications has collaborated with top experts in the field. Together, they have established the Quantum-Safe Internet network, a cybersecurity training center, and the Quantum Communication Center at the University of Vigo. These research initiatives involve companies and universities from various countries, and aim to position Vigo as a key player in the quantum world. The Quantum Communication Center has received nearly $11 million (€10 million) in funding from Spain's Ministry of Science, the regional government of Galicia, and various European research funds, as well as support from companies like Cisco.

Is our current system secure?

To ensure the security of our communications, we rely on cryptographic techniques. These methods are commonly used in applications that connect to the internet and banking services. Whether it's in government, business or military communications, confidentiality is crucial to prevent unauthorized access. With the increasing volume of transmitted information over open networks, protecting data has become more critical than ever. Currently, public key cryptography methods are predominantly used, relying on complex mathematical problems for security. With the advent of quantum computers, many complex problems will become easier to solve, including functions used in cryptography.

Thirty years ago, Peter Shor, a mathematician at the Massachusetts Institute of Technology, cautioned that a quantum computer could efficiently solve factorization problems.

His statement implies that with a quantum computer, all the cryptography currently used on the internet could be broken. One example is factorization, which is a fundamental part of many cryptographic systems. There are other math problems used in cryptography that can also be compromised by a quantum computer. That's why the concept of a Quantum-Safe Internet is important — it focuses on developing strong cryptographic methods to address this challenge.

Is the current development of new security technologies also leading to the emergence of new forms of attack?

With increased computing power, previously challenging problems can become more manageable. Post-quantum cryptography explores tasks that quantum computers may struggle to efficiently solve. Certain algorithms have already been identified and are set to become standard soon, though we can't yet provide guarantees.

In fact, some of the latest algorithms designed to prevent quantum computer attacks have been defeated using classic computers and even laptops.

Yes, those algorithms have advantages, as they enable us to continue using our current infrastructure. However, it's possible that in the future, someone might develop a highly efficient algorithm that can access past data retroactively. Therefore, these solutions are more suitable for short-term applications.

Is there another way?

An alternate solution is based on quantum communications, which offers security against any computer and enables fully secure communications. When you send information over a communication channel that you don't control, it can be copied. However, in quantum mechanics, this isn't possible. When information is encoded in elementary particles in specific states, any attempt to copy it introduces detectable noise. Additionally, unlike conventional methods, there is no certainty that a reproduced copy is authentic. This level of security is independent of computational capacity.

And that's where the University of Vigo comes in?

We've begun a research initiative in Spain and have formed two highly esteemed international groups at the Quantum Communication Center. One group, led by Professor Hugo Zbinden from the University of Geneva, has been at the forefront of quantum communications since the 1990s. They have achieved remarkable breakthroughs and established the current record for maximum transmission distance. The other group, headed by Professor Vadim Makarov of the Quantum Hacking Lab, specializes in certification standards for quantum communication equipment and hacking concerns. While quantum cryptography is absolutely secure in theory, it must be developed very carefully. Makarov is a renowned international expert in identifying and resolving vulnerabilities in these systems.

Is Vigo going to be the capital of quantum security next year?

I'd love to say so. Currently, there are very few or no initiatives in the field of quantum communications that match the talent we have at the University of Vigo.

Could the participation of experts from nations in conflict pose a security issue?

Our work involves conducting research that will be publicly available in scientific publications, so I see no problem with having an international team.

Will there be quantum communications from space?

The European Space Agency has various programs focused on low-orbit satellites. In Spain, the University of Vigo collaborates with Hispasat [the operating company for a number of Spanish communications satellites that cover the Americas, Europe and North Africa] to assess the potential of quantum communication links using high-orbit satellites.

5.Post-Quantum Cryptography Should Be Part of Your Security Strategy

by David G.W. Birch
https://www.forbes.com/sites/davidbirch/2023/08/30/quantum-cryptography-should-be-part-of-your-security-strategy/?sh=243c5c8a15b5

The news that IBM has **used a quantum computer** to solve a problem that that stumps the leading classical methods is another step on the road to what has become known as "quantum advantage", where a quantum system solves a problem that cannot be solved by any amount of classical computation. For those of us in and around fintech, the one problem that we really want to solve is breaking public key cryptography so that we can forge digital signatures, get access to bank systems and, of course, steal a lot of Bitcoin.

Quantum Supremacy

This is important stuff. In the British government's new technology strategy, quantum computing is **one of the "priority" technologies** and it is easy to understand why. That point about solving problems beyond the reach of existing computers means that there is something of an arms race underway, with "quantum supremacy" as the goal.

It will take a while to get to the aforementioned quantum supremacy, where quantum computers can outgun the classical incumbents. But… the IBM solution is already at 127 qubits (quantum bits). If quantum computers are put up against a classical supercomputer capable of up to a quintillion (10^{18}) floating-point operations per second, quantum supremacy **could be reached with as few as 208 qubits**. Quantum supremacy isn't science fiction.

Now, as is well known, one of the interesting problems that a quantum computer can solve is breaking the asymmetric cryptography at the heart of cryptocurrency in order to transfer money out of lost or abandoned wallets. If you look at Bitcoin, for example the accountants Deloitte reckon that about **four million Bitcoins will be vulnerable** to such an attack. That means there are billions of dollars up for grabs in a quantum computing digital dumpster dive.

If we apply quantum computers to the problem of breaking the 256-bit elliptic curve encryption of keys in the Bitcoin network within the small available time frame in which it would actually pose a threat to do so, researchers calculate it would require 317×10^6 physical qubits to break the encryption within one hour using the surface code, a code cycle time of 1 μs, a reaction time of 10 μs, and a physical gate error of 10^{-3}. To instead break the encryption within one day, it would require 13×10^6 physical qubits. So never mind quantum supremacy with a few hundred qubits, quantum computers would need millions of physical qubits to be a threat to Bitcoin.

OK, that's not going to happen tomorrow. Nevertheless, quantum computing will come. So is the sky falling in for the banks and the credit card companies and mobile operators and the military and everyone else who uses public key cryptography then? Well, no. They are not idiots with their heads in the sand and they are already planning to adopt a new generation of Quantum Resistant Cryptographic (QRC) algorithms to defend their data against the inevitable onslaught from quantum computers in unfriendly hands.

They have been looking towards the National Institute of Standards and Technology (NIST), which last year selected a set of algorithms designed to withstand such an onslaught after a six-year effort to devise encryption methods that could resist an attack from a future quantum computer that is more powerful than the comparatively limited machines available today. NIST has now released these algorithms as standards ready for use out in the wild.
(If you are interested in the details, the algorithms are:

CRYSTALS-Kyber, designed for general encryption purposes such as creating secure websites, is covered in FIPS 203;
CRYSTALS-Dilithium, designed to protect the digital signatures we use when signing documents remotely, is covered in FIPS 204;

SPHINCS+, also designed for digital signatures, is covered in FIPS 205;

FALCON, also designed for digital signatures, is slated to receive its own draft FIPS in 2024.)

These algorithms are important because, as noted, while there are no cryptography-breaking quantum computers around right now, they will come. As the quantum technology advances, there will be an inevitable competition between the quantum computers that can break cryptographic algorithms and the cryptography community's efforts to develop quantum-resistant algorithms. This means there will be a period where entities (e.g., Visa and the DoD, not just Bitcoin) will be transitioning to new cryptographic methods.

That period is now, by the way, which is why the US Cybersecurity and Infrastructure Security Agency (CISA) has **just issued a note** calling on critical infrastructure and other organizations to begin work now to create road maps for how they'll migrate to QRC.

(The cryptocurrency world should follow suit so that if and when quantum computers become a threat, then cryptocurrencies can be updated to use QRC. This would be a significant undertaking, but it's theoretically possible.)

Harvest Now, Decrypt Later

Technology strategists in banks, fintechs and "crypto" know why these standard algorithms are being pushed out now, when any actual quantum computer is still some years away. The fact is that you can be at risk from quantum computers that do not yet exist because of what is known as the "**harvest now, decrypt later**" attack. It's the idea that your enemy could copy your data, which is encrypted, and they can hold onto it right now. They can't read it. But maybe when a quantum computer comes out in 10 years, then they can get access to your data.

If the information you're protecting is valuable enough, then you're already in trouble because of that threat and you need to start working on your road map soon.

6.Quantum threats loom in Gartner's 2023 Hype Cycle for data security

by Louis Columbus
https://venturebeat.com/security/whats-new-in-gartners-hype-cycle-for-data-security-in-2023/

The best-run organizations prioritize cybersecurity spending as a business decision first, and Gartner's Hype Cycle for Data Security 2023 reflects the increasing dominance of this approach. Key technologies needed for assessing and quantifying cloud risk are maturing, and new technologies to protect against emerging threats are predicted to gain traction.

Business cases are driving data security integration and technology

Gartner sees the core technologies needed to validate and quantify cyber-risk maturing quickly as more organizations focus on measuring their cybersecurity investments' impact. CISOs tell VentureBeat that it is a new era of financial accountability, and that extends to new technologies for securing data stored in multicloud tech stacks and across networks globally. Getting control of cybersecurity costs is becoming a much higher priority as boards of directors look at how data security spending protects, and potentially grows, revenue.

Gartner's latest Hype Cycle for data security dovetails with what CISOs, CIOs and their teams tell VentureBeat, especially in compliance-centric industries such as insurance, financial services, institutional banking and securities investments. Gartner added five new technologies this year: crypto-agility, post-quantum cryptography, quantum key distribution, sovereign data strategies and digital communications governance. Eight technologies have been removed or reassigned this year.

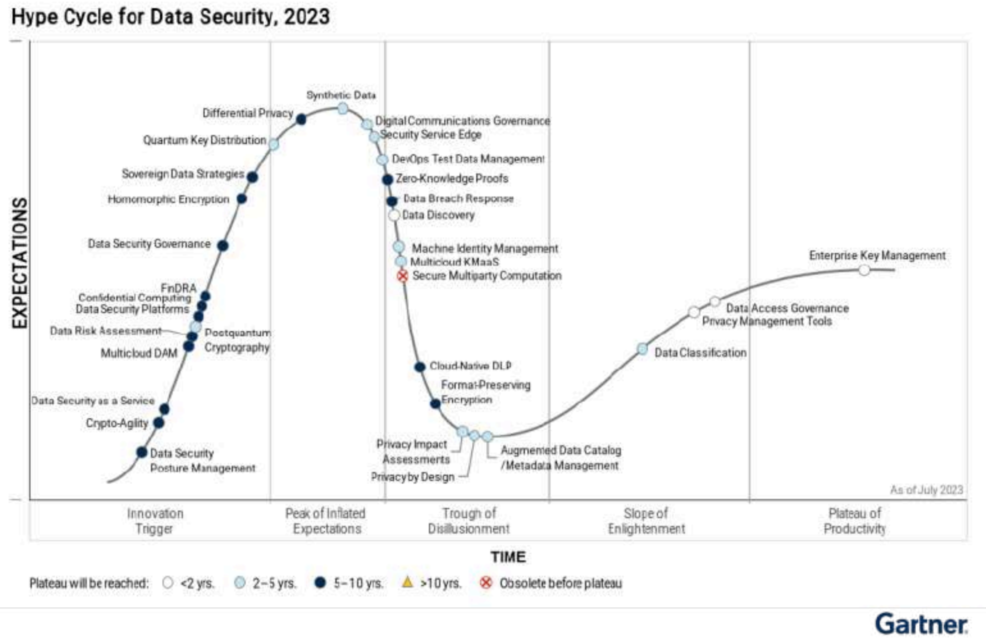
Getting integration right in data security at the enterprise level has always been a challenge. The need for more secure approaches to data integration has led to a proliferation of solutions over the years, some more secure than others. Gartner predicts these challenges will shift or consolidate data security technologies, including data security posture management (DSPM), data security platforms (DSPs) and multicloud database activity monitoring (DAM).

CISOs also say they are monitoring quantum computing as an evolving potential threat and have delegated monitoring it to their strategic IT planning teams. Gartner also introduced crypto-agility in this year's Hype Cycle, responding to its clients' requests for as much data and knowledge as possible in this area.

2023 key trends in data security

CISOs and the teams they manage tell VentureBeat that protecting data in the cloud, and the many identities associated with each data source across multicloud configurations, is getting more challenging given the need to provide access rights by data type while still tracking compliance.

That's made even more difficult by the exponential growth of machine identities across enterprises' cloud instances. This year's Hype Cycle for data security underscores this and other trends summarized here.



Data governance and risk management are now strategic priorities

Board members regularly question CISOs about governance and risk management. CISOs tell VentureBeat that while board members know risk management at an expert level, they need to have the technology-based context of data governance and risk management defined from a tech stack and multicloud perspective.

These dynamics between boards and CISOs are playing out across hundreds of companies as data governance and risk management dominate Gartner's discussions in this year's Hype Cycle. Boards want to know how to accurately quantify cyber-risk, which drives greater compliance. CISOs say that financial data risk assessment (FinDRA) is board-driven and weren't surprised it appears on the Hype Cycle.

Moving data to the cloud increases the need for data-in-use protection technologies

Nearly every business relies on cloud services for a portion, if not all, of their infrastructure and application suites. Gartner sees this as a potential risk for data and has identified a series of technologies and techniques on the Hype Cycle to protect data in use and at rest.

These include confidentiality, homomorphic encryption, differential privacy and secure multiparty computation (SMPC). Confidentiality relies on hardware-based trusted execution environments to isolate data processing, while SMPC allows collaborative data analysis without exposing raw data. The presence of these data-in-use technologies on the Hype Cycle demonstrate the shift from data security at rest to data security in transit.

New quantum computing-based threats on the horizon

Much has been written and predicted about when quantum computing will break encryption. In reality, no one knows when it will happen; however, there's wide consensus that quantum technologies are progressing in that direction. CISOs VentureBeat interviewed on the topic see cryptography at varying levels of urgency depending on their business models, industries and how reliant they are on legacy encryption.

Gartner added both crypto-agility and post-quantum cryptography to the Hype Cycle for the first time this year. CISOs are pragmatic about technologies with as long a runway as these have. In previous interviews, CISOs told VentureBeat they could see where post-quantum cryptography could strengthen zero-trust frameworks in the long term.

New technologies added to the hype cycle

Together, Gartner's five new hype cycle technologies prepare CISOs for the next generation of quantum threats while addressing the most challenging aspects of governance and data sovereignty. The five newly added technologies are briefly summarized here:

- **Crypto-agility**

  The purpose of crypto-agility is to upgrade encryption algorithms used in applications and systems in real time, alleviating the risk of a quantum-based breach. Gartner writes that this will enable organizations to replace vulnerable algorithms with new post-quantum cryptography to ward off attacks using quantum computing to defeat encryption. Crypto-agility offers CISOs a path to secure encryption as quantum capabilities advance over the next five to seven years.

- **Post-quantum cryptography**

  Gartner defines this new technology as based on new quantum-safe algorithms, such as lattice cryptography, that are resistant to decryption by quantum computers. The use case Gartner discusses in the Hype Cycle centers on using this technology in a pre-emptive strategy against quantum-based threats.

  VentureBeat's interviews with CISOs at financial trading firms revealed that pro-forma tech stacks already defend against quantum computing risks and threats. Gartner's latest addition will likely be added to roadmaps for further evaluation by those CISOs responsible for commercial banking and other financial services and institutions. Leading vendors include Amazon, IBM and Microsoft.

- **Quantum key distribution (QKD)**

  This technology works by using quantum physics principles, including photon entanglement, to create and exchange tamper-evident keys. Gartner considers QKD a niche technology today. But given its nature, uses in applications critical to national security are a natural extension of its strengths, as it's anticipated to be useful for exchanging high-value data. Leading vendors include ID Quantique, MagiQ Technologies and Toshiba.

- **Sovereign data strategies**

  This is a new addition to the Hype Cycle that supports data security governance, privacy impact assessment, financial data risk assessment (FinDRA) and data risk assessment. Sovereign data strategies reflect efforts by governments to provide strong governance and data security for their citizens and economy.

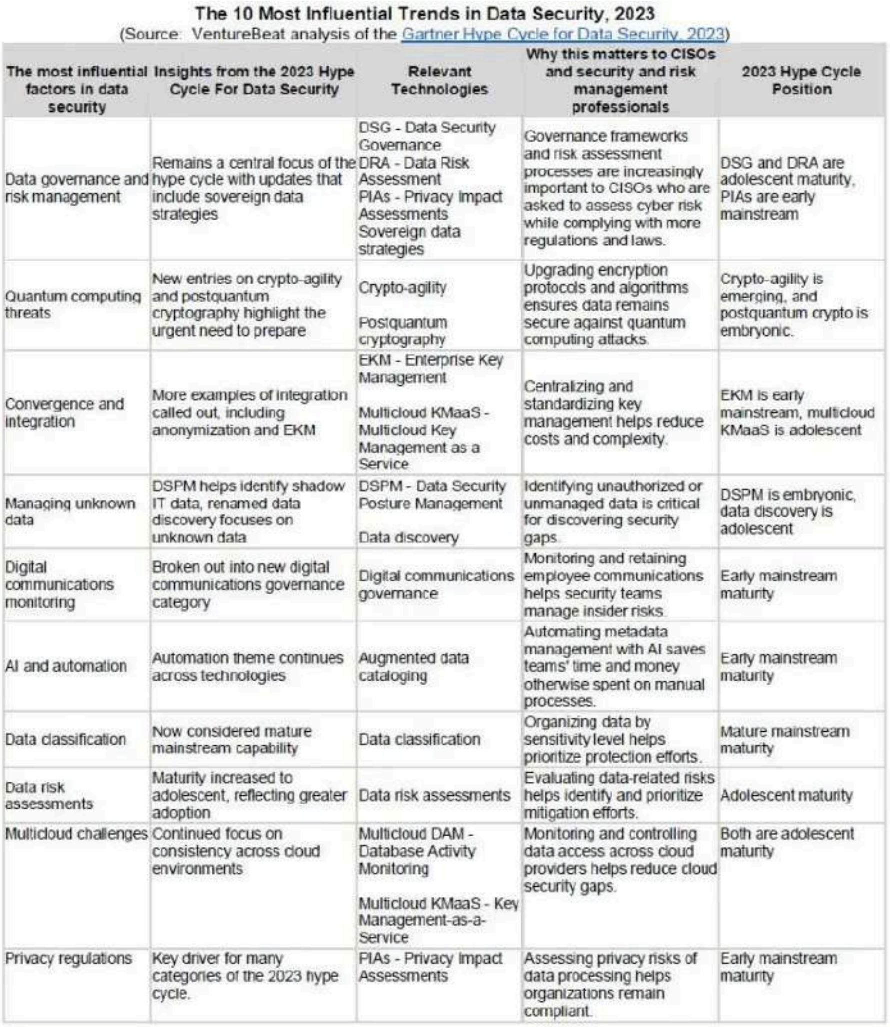
Privacy, security, access, use, retention, sharing regulations, processing and persistence are examples cited by Gartner. According to the firm, sovereign data strategies will eventually become table stakes for any business that needs to complete transactions across sovereign jurisdictions.

- **Digital communications governance**

  Digital communications governance (DCG) solutions monitor, analyze and enforce employee messaging, voice and video compliance policies. DCG platforms also manage regulatory and corporate governance requirements with data retention, surveillance, behavioral analytics and e-discovery. They help compliance teams identify misconduct and comply with regulations by monitoring communications data.

  DCG also helps CIOs and CISOs manage employee messaging, voice and video platform risks by consolidating access and enforcement across communication channels. Leading vendors include Global Relay, Proof-point and Veritas.

Trends most strongly driving the future of data security



The 10 Most Influential Trends in Data Security, 2023
(Source: VentureBeat analysis of the Gartner Hype Cycle for Data Security, 2023)

The most influential factors in data security	Insights from the 2023 Hype Cycle For Data Security	Relevant Technologies	Why this matters to CISOs and security and risk management professionals	2023 Hype Cycle Position
Data governance and risk management	Remains a central focus of the hype cycle with updates that include sovereign data strategies	DSG - Data Security Governance DRA - Data Risk Assessment PIAs - Privacy Impact Assessments Sovereign data strategies	Governance frameworks and risk assessment processes are increasingly important to CISOs who are asked to assess cyber risk while complying with more regulations and laws.	DSG and DRA are adolescent maturity, PIAs are early mainstream
Quantum computing threats	New entries on crypto-agility and postquantum cryptography highlight the urgent need to prepare	Crypto-agility Postquantum cryptography	Upgrading encryption protocols and algorithms ensures data remains secure against quantum computing attacks.	Crypto-agility is emerging, and postquantum crypto is embryonic.
Convergence and integration	More examples of integration called out, including anonymization and EKM	EKM - Enterprise Key Management Multicloud KMaaS - Multicloud Key Management as a Service	Centralizing and standardizing key management helps reduce costs and complexity.	EKM is early mainstream, multicloud KMaaS is adolescent
Managing unknown data	DSPM helps identify shadow IT data, renamed data discovery focuses on unknown data	DSPM - Data Security Posture Management Data discovery	Identifying unauthorized or unmanaged data is critical for discovering security gaps.	DSPM is embryonic, data discovery is adolescent
Digital communications monitoring	Broken out into new digital communications governance category	Digital communications governance	Monitoring and retaining employee communications helps security teams manage insider risks.	Early mainstream maturity
AI and automation	Automation theme continues across technologies	Augmented data cataloging	Automating metadata management with AI saves teams' time and money otherwise spent on manual processes.	Early mainstream maturity
Data classification	Now considered mature mainstream capability	Data classification	Organizing data by sensitivity level helps prioritize protection efforts.	Mature mainstream maturity
Data risk assessments	Maturity increased to adolescent, reflecting greater adoption	Data risk assessments	Evaluating data-related risks helps identify and prioritize mitigation efforts.	Adolescent maturity
Multicloud challenges	Continued focus on consistency across cloud environments	Multicloud DAM - Database Activity Monitoring Multicloud KMaaS - Key Management-as-a-Service	Monitoring and controlling data access across cloud providers helps reduce cloud security gaps.	Both are adolescent maturity
Privacy regulations	Key driver for many categories of the 2023 hype cycle.	PIAs - Privacy Impact Assessments	Assessing privacy risks of data processing helps organizations remain compliant.	Early mainstream maturity

Ten key trends emerge from this year's Hype Cycle. Data governance, risk management and compliance are core drivers of the data security market. Gartner believes that preparing for quantum computing threats, convergence and integration of security tools, and managing unknown shadow IT data are high priorities.

The above matrix compares the most influential factors, in order of priority, that are influencing the future of data security.

7.Innovative Atomic Device Enables a Simpler Way to Connect Quantum Computers

by Princeton University
https://scitechdaily.com/innovative-atomic-device-enables-a-simpler-way-to-connect-quantum-computers/?expand_article=1#google_vignette

A new atomic device sends high-fidelity quantum information over fiber optic networks.

Researchers have unveiled a new way to connect quantum devices over long distances, a necessary step toward allowing the technology to play a role in future communications systems.

While today's classical data signals can get amplified across a city or an ocean, quantum signals cannot. They must be repeated in intervals — that is, stopped, copied, and passed on by specialized machines called quantum repeaters. Many experts believe these quantum repeaters will play a key role in future communication networks, allowing enhanced security and enabling connections between remote quantum computers.

New Approach to Quantum Repeaters

The Princeton study, published today (August 30) in *Nature*, details the basis for a new approach to building quantum repeaters. It sends telecom-ready light emitted from a single ion implanted in a crystal. The effort was many years in the making, according to Jeff Thompson, the study's principal author. The work combined advances in photonic design and materials science.

Other leading quantum repeater designs emit light in the visible spectrum, which degrades quickly over optical fiber and must be converted before traveling long distances. The new device is based on a single rare earth ion implanted in a host crystal. And because this ion emits light at an ideal infrared wavelength, it requires no such signal conversion, which can lead to simpler and more robust networks.

Device Design and Functionality

The device has two parts: a calcium tungstate crystal doped with just a handful of erbium ions, and a nanoscopic piece of silicon etched into a J-shaped channel. Pulsed with a special laser, the ion emits light up through the crystal. But the silicon piece, a whisp of a semiconductor stuck onto the top of the crystal, catches and guides individual photons out into the fiber optic cable.

Ideally, this photon would be encoded with information from the ion, Thompson said. Or more specifically, from a quantum property of the ion called spin. In a quantum repeater, collecting and interfering the signals from distant nodes would create entanglement between their spins, allowing end-to-end transmission of quantum states despite losses along the way.

Material Selection and Testing

Thompson's team first started working with erbium ions several years before, but the first versions used different crystals that harbored too much noise. In particular, this noise caused the frequency of the emitted photons to jump around randomly in a process known as spectral diffusion. This prevented the delicate quantum interference that is necessary to operate quantum networks. To solve this problem, his lab started working with Nathalie de Leon, associate professor of electrical and computer engineering, and Robert Cava, a leading solid-state materials scientist and Princeton's Russell Wellman Moore Professor of Chemistry, to explore new materials that could host single erbium ions with much less noise.

They winnowed the list of candidate materials from hundreds of thousands down to a few hundred, then a couple dozen, then three. Each of the three finalists took half a year to test. The first material turned out to be not quite clear enough. The second caused the erbium to have poor quantum properties. But the third, the calcium tungstate, was just right.

Proving the New Material's Potential

To demonstrate that the new material is suitable for quantum networks, the researchers built an interferometer where photons randomly pass through one of two paths: a short path that is several feet long, or a long path that is 22 miles long (made of spooled optical fiber). Photons emitted from the ion can go on the long path or the short path, and about half the time, consecutive photons take opposite paths, and arrive at the output at the same time.

When such a collision occurs, quantum interference causes the photons to leave the output in pairs if and only if they are fundamentally indistinguishable – having the same shape and frequency. Otherwise, they leave the interferometer individually. By observing a strong suppression — up to 80 percent — of individual photons at the interferometer output, the team proved conclusively that the erbium ions in the new material emit indistinguishable photons. According to Salim Ourari, a graduate student who co-led the research, that puts the signal well above the hi-fi threshold.

Future Work

While this work crosses an important threshold, additional work is required to improve the storage time of quantum states in the spin of the erbium ion. The team is currently working on making more highly refined calcium tungstate, with fewer impurities that disturb the quantum spin states.

8.IBM makes major leap in quantum computing error-detection

by Peter Grad
https://phys.org/news/2023-08-ibm-major-quantum-error-detection.html

Quantum computing is on the verge of catapulting the digital revolution to new heights.

Turbocharged processing holds the promise of instantaneously diagnosing health ailments and providing rapid development of new medicines; greatly speeding up response time in AI systems for such time-sensitive operations as autonomous driving and space travel; optimizing traffic control in congested cities; helping aircraft better navigate extreme turbulence; speeding up weather forecasting that better prepares localities facing potential disaster, and optimizing supply chain systems for more efficient delivery times and cost savings.

But we're not there yet. One of the greatest obstacles facing quantum operations is error-correction.

The price for speedier operations in quantum systems is a higher error rate. Quantum computers are highly susceptible to noise such as electromagnetic signals, temperature change and disturbances in the Earth's magnetic field. Such noise triggers errors.

Qubits, the components particular to quantum computing, themselves are prone to error. Faults in frequencies, energy levels and coupling strength can cause miscalculations.

Unlike standard computer bits that are copied reliably most of the time, qubits, by their very nature, cannot be cloned without errors being introduced. Bits store easily replicated binary digit states while qubits store data in a complex mathematical quantum state that can be disrupted during copying. Additionally, qubits age quickly and deterioration can introduce errors.

Researchers at IBM Quantum say they have developed a system that dramatically improves error-detection in quantum computing. In an online post Aug. 28, they explained the challenge: "Standard classical error-correction only needs to correct bit flip errors," said IBM researcher Sergey Bravyi.

"Quantum computers must correct more kinds of errors, like phase errors which can corrupt the extra quantum information that qubits carry … Techniques must [also] correct errors without the ability to copy unknown quantum states, and without destroying the underlying quantum state.”

In their research paper, IBM researchers described a process they say greatly trims the required arsenal currently used in quantum computing to catch errors.

Standard computer surface codes have long been successfully used for error-corrections. These are two-dimensional grids resembling a checkerboard. Efficient error-correction for qubits is more challenging.

Bravyi says many experts estimate fault-tolerant quantum computing would require millions of qubits, "a number we believe is too large to be practical at this stage of development.”

IBM's solution, improved code and a redesign of qubit placement, achieves results requiring one-tenth the number of physical qubits currently used in error-correction.

"Practical error correction is far from a solved problem," the researchers acknowledged in a paper titled "High-threshold and low-overhead fault-tolerant quantum memory" published Aug. 15 in the preprint server *arXiv*.

"However, these new codes and other advances across the field are increasing our confidence that fault tolerant quantum computing isn't just possible, but is possible without having to build an unreasonably large quantum computer.”

Their approach currently only works on quantum memory and not computational power.

"These techniques are a stepping stone towards a world of fault-tolerant computing," Bravyi says, "and this new … code is bringing that world closer. It's a promising result pointing us where we should look next for even better error correcting codes."

9.How India became the hottest date in quantum computing

by Stephanie Stacey
https://techmonitor.ai/hardware/quantum/how-india-became-the-hottest-date-in-quantum-computing

Professor Bhupendra Dev got an exciting delivery in May: an ultra-low temperature dilution refrigerator built by a Finnish company Bluefors. It suited Dev's purposes perfectly. The device will, the professor explains, provide temperatures close to absolute zero (-273.15°C) — a stark contrast from the tropical climate on the streets outside the researcher's lab in Kolkata, India. “People sometimes joke that Finland is a cold country and that's why they can provide the refrigeration systems,” says Dev.

The icy extremes are essential for Dev's research at the Centre for Quantum Engineering, Research and Education (CQuERE), where he's trying to build one of India's first quantum computers. Most of the electronics are already in place, except for a few couplers, and Dev hopes to begin working with his first qubit — the basic unit of quantum information — in about six months. “We'll proceed pretty slowly, because at this stage [we] have to train the students,” says Dev.

Although it's still in development, quantum computers have the potential to perform complex calculations exponentially faster than their so-called ‘classical’ counterparts. As such, these exotic devices could accelerate scientific breakthroughs and streamline supply chains, as well as enhance navigation and detection systems and offering a fool-proof form of encryption. That's why there's such a dash to uncover its secrets: the nations that manage to harness the technology first will, naturally, be the first to reap its promised rewards.

More ominous, however, is the fact that quantum computers' speedy mathematical prowess could enable them to completely overwhelm our existing encryption standards — a pivotal event that researchers call ‘Q-Day.’ “If it works, it will change everything,” says Emily Harding, a senior fellow on the CSIS International Security Program. “Anything from secret government communications to bank transactions could, in theory, be decrypted by a functioning quantum computer.”

Quantum, therefore, is increasingly seen as a game-changer — both for economic development and for international security. As such, the latent technology is already turning into a geopolitical minefield, even before many of its ambitious promises come to fruition. India, which has previously lagged behind other nations in the field, is frantically trying to leapfrog its competitors, especially in light of its growing fear of China. The country is charting an ambitious path — backed by a hefty package of government funding and an extensive catalogue of collaborations with researchers scattered across the globe.

India's National Quantum Mission

On April 19, 2023, India's federal government approved a $730mn funding package for the country's inaugural National Quantum Mission (NQM). The project aims to deliver intermediate-scale quantum computers with 50-1,000 physical qubits by 2031 and “make India one of the leading nations in the development of Quantum Technologies & Applications (QTA).”

India's government says that the programme – which covers everything from homegrown quantum computing capacities to Quantum Key Distribution (QKD), and quantum sensing – will boost sectors like communications and health. It's also sure to be harnessed to enhance the nation's military capacities. Specifically, India is also hoping to enable satellite-based secure quantum communications over a range of 2,000 km, as well as building intercity, land-based, QKD capacities over the same distance. That would be a big advance on the nation's existing capacities. In 2022, local start-up QNU Labs, which worked alongside the Indian Army on the project, announced it could share encrypted keys over distances of up to 150 km.

India's current push for quantum development makes a lot of sense, says Harding. The country has both a wealth of technical expertise and the drive – spurred by concerns about China – to channel this expertise towards quantum innovation. There are also plenty of avenues for international collaboration, including with global leaders like the US, which has been actively exploring numerous avenues to boost its collaboration with India.

Nevertheless, she says, it's not surprising that it's taken so long for India to get off the ground with its National Quantum Mission. "It's very hard to energise a gigantic government towards a threat that's theoretical," says Harding. There's also a pretty hefty price tag on this kind of work, "so much so that you see the huge companies and big wealthy countries being the ones who are really pursuing it."

India's goals are ambitious, certainly, but researchers at CQuERE, say they're also trying to chart their own path. "The important thing is that we are not going to be in a rat race for making a larger computer with more qubits," says Dev. That would be a losing battle – especially given the mighty advantages of US giants like IBM, which has already set its sights on building a whopping 100,000-qubit machine by 2033. "We are concentrating on making a small computer with fewer qubits," says Dev.

India is starting on the back foot, so it'll need to do things differently if it doesn't want to be stuck forever playing catch-up, agrees Professor Bhanu Das, director of CQuERE. "We will have to think about new problems, novel applications, which will have an impact," says Das. "If we just repeat what others have done in different countries, that's not going to be very helpful."

Making friends

India has explicitly identified quantum computing as an area for international collaboration and knowledge-sharing. To that end, the country has already forged major partnerships through the US-India Initiative for Critical Emerging Technologies (IcET), and the EU-India Trade and Technology Council (TTC). It has also received individual overtures from prominent figures everywhere from Singapore to Finland.

Scientists in India stand to benefit from the country's relatively friendly relationship with the West, unlike their counterparts in Russia or China. "China may be ahead of India in this field, but China will not be able to collaborate with many countries, especially the US and Europe," says Das. "The fact that India can collaborate, both in research and education, with the US, Europe, Japan, and Australia is a huge advantage – and in our research centre we will do our best to benefit from this situation."

Indeed, CQuERE has already built major partnerships with the University of Tokyo and Keio University in Japan, the University of Wisconsin, and Spanish start-up Qilimanjaro. These partnerships, says Das, are "absolutely important" – both because the field is fairly new, and because India has "sort of lagged behind." By teaming up with teams overseas, Das's group has already been able to conduct experiments on existing quantum computers in the US and Japan – even before building their own. "We work with people who have actually built quantum computers, so the quantum computer is not a black box for us," says Das.

India is also being courted by researchers from Russia – many of whom have lost existing scientific partnerships with Europe and the US amid Russia's brutal war in Ukraine. This isn't the first time that Delhi and Moscow have joined forces on technology. After the 1971 Indo-Soviet Friendship Treaty, India and the Soviet Union cooperated closely on everything from nuclear development to space launches (India's first satellite, Aryabhata, was launched from the Russian launch complex at Kapustin Yar in 1975.) This technological cooperation hasn't dimmed in the decades since the collapse of the Soviet Union – notwithstanding the emergence of some fault-lines in recent years as India has started to draw closer to the US.

Ruslan Yunusov, co-founder of Russian Quantum Centre (RQC), recently told reporters that he's keen to promote a collaborative quantum lab under the BRICS group of nations, which currently comprises Brazil, Russia, India, China and South Africa (and will soon expand). "There are no signed contracts yet, but India has done a lot of work around quantum technology," said Yunusov, speaking from the sidelines of the Future Technologies Forum in Moscow, which was attended by President Vladimir Putin. "We are already in talks with some research institutes in India to explore areas where we can use their expertise and also share our knowledge and work in the field."

Beyond its non-aligned status, which has helped it score a wide array of international partnerships, there are several key factors on India's side. The country has a large — and growing – start-up ecosystem, so emerging scientific research can quickly find a practical (and profitable) home, says researcher Achyut Chandra. It also has a very large pool of students – a group that, according to Das, could be the country's greatest asset. "If that can be taken advantage of," he says, "then I think India has a good future in this field."

Sharing might be central to India's growth in quantum computing — but how long can this go on? "Scientists are scientists, and they're wonderful human beings, and they love to share scientific knowledge," says Harding. "It's people like me who are focused on the security aspects of it, who come to the party and say: 'Now let's slow down. Let's not share all our scientific achievements with our potential competitors.' I tend to get booed out of the room when that happens."

Booing aside, Harding's concerns are shared in Washington. Leaders in the US, she says, have already started asking at what point export controls or security classifications might be deemed prudent for quantum devices. "I don't have an answer to that question," concedes Harding. Nevertheless, she says, it's "one that I think governments are going to struggle with mightily in the next couple of years."

For now, though, could India's web of international alliances be enough to help the country catch up with its more advanced competitors — at least in terms of efficiency and innovation, if not in the sheer might of its quantum devices? "I'm cautiously optimistic," says Das. "I think we have the human power. […] If we plan things well, both in research and education, I think India can be successful."

10.NIST Publishes First Draft Standards for Post-Quantum Cryptography

by Jeffrey Schwartz

https://www.darkreading.com/dr-tech/nist-publishes-first-draft-standards-for-post-quantum-cryptography

The first draft standards for quantum-resistant public key cryptography based on algorithms chosen by the National Institute for Standards and Technology (NIST) are now available for public comment.

On Aug. 24, NIST published three of the four algorithms that the standards body selected last year: Crystals-Kyber, Crystals-Dilithium, and Sphincs+. The formal names of the draft standards will be known respectively as ML-KEM, ML-DSA, and SLH-DSA, NIST revealed. Because the fourth algorithm, Falcon, requires significantly more complex computation, NIST is aiming to publish that draft standard, to be named NL-DSA, early next year.

The publication of NIST's first post-quantum cryptographic (PQC) draft standards marks an important milestone in its effort, launched in 2016, to address the potential for quantum computers to break existing RSA encryption and elliptic-curve cryptography (ECC).

The release of the draft standard opens 90 days for public comment, says Dustin Moody, a mathematician at NIST who leads its PQC standardization project.

"Hopefully, within a few months after that, we'll be able to make any changes and publish the finalized versions of the standards," Moody says.

The release of the drafts sets the stage for the Internet Engineering Task Force (IETF) to focus on interoperability, adds Tim Hollebeek, industry and technical standards strategist at DigiCert.

"People can now see what we want to use for key exchange and key encapsulation, which is Kyber, and we now know that Dilithium will be the primary signing algorithm that we'll be using," says Hollebeek, who co-chairs the IETF's Limited Additional Mechanisms for PKIX and SMIME (LAMPS) working group.

PQC Implementation Testing to Begin

With the release of the draft standards, engineers can start working on prototypes of various capabilities, such as how secure email and the implementation of TLS might work in the future, Hollebeek says.

"One of the important things about asymmetric cryptography is the entire use case is around two people trying to communicate with each other securely," he says.

During a live workshop last week at NIST's National Cybersecurity Center of Excellence (NCCoE) — its first live gathering since the pandemic — Hollebeek participated in a panel discussion on interoperability.

"We need to know that everybody's implementation of the protocols will work correctly with everybody else's implementation of the protocols," he said

Looking ahead, various stakeholders will gather in November for hackathons in advance of the next IETF meeting in Prague, where they will test each other's implementations of the PQC draft standards.

"We're working together with some of our competitors and some of our friends on making sure that our reading of the standards and their readings of the standards agree," Hollebeek says. "And a lot of times when people find out that the implementations don't interoperate with each other, what it does is it points out ambiguities in the standard — things that people didn't specify correctly."

Among those that will work with vendors such as DigiCert and Entrust is PKI provider Keyfactor, whose co-founder and CTO, Ted Shorter, says ensuring interoperability is complex.

"All these algorithms have different parameters, key lengths, and exponent sizes, and all these different things that you can use as a part of a cryptographic algorithm," Shorter says. "And there's different parameter sets that must be considered."

Shorter says the four algorithms selected by NIST are now supported in the open source project it sponsors. Bouncy Castle includes a set of lightweight cryptographic APIs for Java and C#, as well as providers for the Java Cryptography Extension (JCE), Java Cryptography Architecture (JCA), and Java Secure Socket Extension (JSSE).

Call for More Signature Algorithms

Building on the four algorithms that will become the first PQC standards, NIST put out a calllast September for additional digital signature proposals — specifically not based on structure lattices. NIST requested algorithms with short signatures that enable rapid verification for applications, such as certificate transparency.

NIST emphasized that any structured lattice-based signature proposal must substantially outperform Dilithium and Falcon. Moody says NIST received 50 submissions, 40 of which met the criteria for consideration.

Fears that quantum computers could break current encryption began to emerge in 1994 when MIT professor Peter Shor famously described how a quantum computer could easily do so. Unlike conventional computers, which process ones and zeros to perform calculations, quantum computers use qubits, described as subatomic particles, such as electrons or photons.

Only a handful of companies claim the resources to develop quantum computers; several have revealed advances in recent years. Among those that have revealed their quantum computing capabilities are IBM, Google, Microsoft, and Quantinuum, a company spun out of Honeywell.

Experts in computing, cybersecurity, and physics have debated for some time when a quantum computer capable of running what is known as Shor's algorithm can break current encryption. No one knows when a commercially viable quantum computer will emerge because it will require breakthroughs in physics yet to be achieved.

Still, many experts predict quantum computing capability could surface within the next decade. Some say it could happen sooner, while others see no time frame. Perhaps the most notable skeptic is famous cryptographer Adi Shamir.

During the Cryptographers Panel at this year's RSA Conference, Shamir gave what he admitted was a harsh view.

"I must say that the main things which have been delivered are more promises, and as of today, not a single practical problem has been shown to be solvable by one of the available quantum computers faster than on a classical computer," he said.

Although Shamir didn't suggest that quantum computers would never be a threat to cryptography, he said a usable system could be 30 or more years in the future. Nevertheless, Shamir conceded, "Using older algorithms such as RSA or elliptic curves might become decryptable in the future."

However, many believe a quantum system that could break existing encryption could surface within the next decade; the National Security Agency (NSA) shares those concerns. In September 2022, the NSA announced a migration path from the current Commercial National Security Algorithm (CNSA) Suite 1.0, which includes the 256-bit Advanced Encryption Standard (AES), Elliptic-curve Diffie–Hellman, and the Elliptic Curve Digital Signature Algorithm.

Bringing more urgency to the debate, late last year US President Joe Biden signed the Quantum Computing Cybersecurity Preparedness Act into law, directing the Office of Management and Budget (OMB) to implement the NIST-approved cryptographic algorithms.

In September 2022, the NSA issued an order mandating government agencies to ensure all of their systems are migrated to the NIST-selected quantum-resistant algorithms by 2035.

While it may be an ambitious goal, NIST's Moody believes it's a reasonable path.

"We're trying to help get this transition migration happening as quickly as possible," Moody says. "Crypto transitions always take way longer than we expect or want them to. We're glad that they're trying to make sure agencies are going as fast as they can."

11.NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers

by Chad Boutin
https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

Three new algorithms are expected to be ready for use in 2024. Others will follow.

Last year, the National Institute of Standards and Technology (NIST) selected four algorithms designed to withstand attack by quantum computers. Now the agency has begun the process of standardizing these algorithms — the final step before making these mathematical tools available so that organizations around the world can integrate them into their encryption infrastructure.

Today NIST released draft standards for three of the four algorithms it selected in 2022. A draft standard for FALCON, the fourth algorithm, will be released in about a year.

NIST is calling on the worldwide cryptographic community to provide feedback on the draft standards until Nov. 22, 2023.

“We’re getting close to the light at the end of the tunnel, where people will have standards they can use in practice,” said Dustin Moody, a NIST mathematician and leader of the project. “For the moment, we are requesting feedback on the drafts. Do we need to change anything, and have we missed anything?”

Sensitive electronic information, such as email and bank transfers, is currently protected using public-key encryption techniques, which are based on math problems a conventional computer cannot readily solve. Quantum computers are still in their infancy, but a sufficiently powerful one could solve these problems, defeating the encryption. The new standards, once completed, will provide the world with its first tools to protect sensitive information from this new kind of threat.

A Multiyear Evaluation Process

NIST’s effort to develop quantum-resistant algorithms began in 2016, when the agency called on the world’s cryptographic experts to submit candidate algorithms to NIST’s Post-Quantum Cryptography Standardization Project. Experts from dozens of countries submitted 69 eligible algorithms by the November 2017 deadline.

NIST then released the 69 candidate algorithms for experts to analyze, and to crack if they could. This process was open and transparent, and many of the world’s best cryptographers participated in multiple rounds of evaluation, which reduced the number of candidates.

Although quantum computers powerful enough to defeat current encryption algorithms do not yet exist, security experts say that it’s important to plan ahead, in part because it takes years to integrate new algorithms across all computer systems.

Each new publication is a draft Federal Information Processing Standard (FIPS) concerning one of the four algorithms NIST selected in July 2022:

- **CRYSTALS-Kyber**, designed for general encryption purposes such as creating secure websites, is covered in FIPS 203.
- **CRYSTALS-Dilithium**, designed to protect the digital signatures we use when signing documents remotely, is covered in FIPS 204.
- **SPHINCS+**, also designed for digital signatures, is covered in FIPS 205.
- **FALCON**, also designed for digital signatures, is slated to receive its own draft FIPS in 2024.

The publications provide details that will help users implement the algorithms in their own systems, such as a full technical specification of the algorithms and notes for effective implementation. Additional guidance will be forthcoming in companion publications, Moody said.

Additional Algorithm Standards

While these three will constitute the first group of post-quantum encryption standards NIST creates, they will not be the last.

In addition to the four algorithms NIST selected last year, the project team also selected a second set of algorithms for ongoing evaluation, intended to augment the first set. NIST will publish draft standards next year for any of these algorithms selected for standardization. These additional algorithms — likely one or two, Moody said — are designed for general encryption, but they are based on different math problems than CRYSTALS-Kyber, and they will offer alternative defense methods should one of the selected algorithms show a weakness in the future.

This need for backups was underscored last year when an algorithm that initially was a member of the second set proved vulnerable: Experts outside NIST cracked SIKE with a conventional computer. Moody said that the break was unusual only in that it came relatively late in the evaluation process. “It was mainly an indication that our process is working as it should,” he said.

The team members also want to make sure they have considered all the latest ideas for post-quantum cryptography, particularly for digital signatures. Two of the three post-quantum methods for digital signatures selected thus far are based on a single mathematical idea called structured lattices. Should any weaknesses in structured lattices emerge, it would be helpful to develop additional approaches that are based on other ideas. The NIST team recently requested submissions of additional signature algorithms that cryptographers have designed since the initial 2017 submission deadline, and the team plans to evaluate these submissions through a multi-round public program to be conducted over the next few years. The 40 submissions that met the acceptance criteria are posted here.

Eventually, the completed post-quantum encryption standards will replace three NIST cryptographic standards and guidelines that are the most vulnerable to quantum computers: FIPS 186-5, NIST SP 800-56A and NIST SP 800-56B.

NIST is accepting feedback from the public on the FIPS 203, 204 and 205 draft standards until Nov. 22, 2023.

12.Advances in Quantum Emitters Mark Progress Toward a Quantum Internet

by Matt Swayne
https://thequantuminsider.com/2023/08/23/advances-in-quantum-emitters-mark-progress-toward-a-quantum-internet/

The prospect of a quantum internet, connecting quantum computers and capable of highly secure data transmission, is enticing, but making it poses a formidable challenge. Transporting quantum information requires working with individual photons rather than the light sources used in conventional fiber optic networks. To produce and manipulate individual photons, scientists are turning to quantum light emitters, also known as color centers. These atomic-scale defects in semiconductor materials can emit single photons of fixed wavelength or color and allow photons to interact with electron spin properties in controlled ways.

A team of researchers has recently demonstrated a more effective technique for creating quantum emitters using pulsed ion beams, deepening our understanding of how quantum emitters are formed. The work was led by Department of Energy Lawrence Berkeley National Laboratory (Berkeley Lab) researchers Thomas Schenkel, Liang Tan, and Boubacar Kanté who is also an associate professor of electrical engineering and computer sciences at the University of California, Berkeley. The results appeared in *Physical Review Applied* and are part of a larger effort by the team to identify the best quantum defect emitters for processing and transporting quantum information and to produce them with precision.

“The color centers we’re making are candidates for becoming the backbone of a quantum internet and a key resource for scalable quantum information processing,” said Schenkel, a senior scientist in Berkeley Lab’s Accelerator Technology & Applied Physics (ATAP) Division. “They could support linking quantum-computing nodes for scalable quantum computing.”

In this work, the team targeted the fabrication of a specific type of color center in silicon comprising two substitutional carbon atoms and a slightly dislodged silicon atom. The conventional method of producing the defects is to hit the silicon with a continuous beam of high-energy ions; however, the researchers discovered that a pulsed ion beam is significantly more efficient, producing many more of the desired color centers.

“We were surprised to find these defects can be more easily generated with pulsed ion beams,” said Wei Liu, a postdoctoral scholar in ATAP and first author of the publication. “Right now, industry and academia mainly use continuous beams, but we’ve demonstrated a more efficient approach.”

The researchers believe that the transient excitations created by the pulsed beam, where the temperature and system energetics change rapidly, are key to the more efficient color center formation, which they established through an earlier study using pulsed ion beams from a laser-driven accelerator published in *Communications Materials*.

The team characterized the color centers at cryogenic temperatures using highly sensitive near-infrared detectors to probe their optical signals. They found that the intensity of the ion beam used to create the color centers changed the optical properties of the photons they emitted. Large-scale computer simulations on the *Perlmutter* system at the National Energy Research Scientific Computing Center (NERSC) provided further insight into the discovery, revealing that the wavelength of emitted photons is sensitive to strain in the crystal lattice.

“First-principles electronic structure calculations have become the go-to method for understanding defect properties,” added Vsevolod Ivanov, a postdoctoral scholar at the Molecular Foundry and co-first author of the publication. “We have reached the point where we can predict how a defect behaves, even in complex environments.”

The findings also suggest a new application for quantum emitter color centers as sensors for radiation.

“It opens new directions,” said Tan, a staff scientist at Berkeley Lab’s Molecular Foundry. “We can form this color center by just hitting silicon with a proton. We could potentially use that as a dark-matter or neutrino detector with directionality because we see these different strain fields depending on which way the radiation came.”

With this deeper understanding of quantum emitter formation and properties, the team continues to expand its exploration of color centers. Ongoing work includes generating a database of color centers predicted to exist in silicon, using computer simulations to identify those best suited to quantum computing and networking applications, and refining fabrication techniques to gain deterministic control over creating individual color centers.

“We’re working towards a new paradigm of qubits by design,” said Kanté. “Can we reliably make a given color center that operates in the telecom band, has sufficient brightness, isn’t too hard to make, has a memory, etcetera? We’re engaged in that quest and have demonstrated some exciting progress.”

“The new pathways to forming color centers using intense beams uncovered in this work are an exciting application of high energy density conditions and plasma science to improving technologies for quantum information science,” said ATAP Division Director Cameron Geddes.

The Molecular Foundry and National Energy Research Scientific Computing Center (NERSC) are DOE Office of Science user facilities located at Berkeley Lab.

This research was funded by the DOE Office of Science’s Fusion Energy Sciences and High Energy Physics programs.

13.Rambus boosts FPGA security with post quantum IP

by Nick Flaherty
https://www.eenewseurope.com/en/rambus-boosts-fpga-security-with-post-quantum-ip/

Rambus has launched a suite of security IP for the FPGA market with the latest cryptographic, side-channel and Quantum Safe protections.

The Rambus security IP is designed to be integrated into FPGAs used in Data Centre, Artificial Intelligence / Machine Learning, Edge, IoT and Defence applications.

The IP blocks covers root of trust, 800G MACsec, IPsec and classic and quantum safe public key encryption designs. These have been designed with differential power analysis (DPA) and fault injection attack (FIA) countermeasures to prevent side channel attacks where hackers analyse the power and thermal changes to determine the security keys.

The blocks also implement coming Post Quantum Cryptography (PQC) requirements with new algorithms and approaches that would take even future quantum computers many years to crack.

- Algorithms agreed for post-quantum security standard
- CryptoManager Root of Trust cores certified to ASIL-B/D

“As customer demand for security continues to accelerate, Rambus is dedicated to providing security IP for the broad range of applications increasingly enabled by FPGAs,” said Neeraj Paliwal, general manager of Silicon IP at Rambus. “Our security IP solutions safeguard these FPGA devices now and in the future with Quantum Safe protection from PQC attacks.”

“In the increasingly distributed and accelerator-based computing architectures enabled by Intel FPGAs, it is mission critical to secure data and devices against today’s threats and those that arise with the advent of quantum computing,” said Premal Buch, vice president and general manager of Programmable Solutions at Intel. “We’re pleased to see Rambus offer security IP solutions tailored to FPGAs powering the growing landscape of accelerated computing.

- Rambus sells its PHY business to Cadence
- Rambus takes aim at ARM in IoT security

Rambus is in the process of selling its connectivity PHY IP to Cadence Design Systems to focus on other IP.

14.Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and National Institute of Standards and Technology (NIST) warned that cyber actors could target our nation’s most sensitive information now and leverage future quantum computing technology to break traditional non-quantum-resistant cryptographic algorithms. This could be particularly devastating to sensitive information with long-term secrecy requirements.

The joint Cybersecurity Information Sheet (CSI), “Quantum-Readiness: Migration to Post-Quantum Cryptography,” helps the Department of Defense, National Security System (NSS) owners, the Defense Industrial Base (DIB), and others proactively protect the confidentiality, integrity, and authenticity of sensitive information.

“Post-quantum cryptography is about proactively developing and building capabilities to secure critical information and systems from being compromised through the use of quantum computers,” said Rob Joyce, Director of NSA Cybersecurity. “The transition to a secured quantum computing era is a long-term intensive community effort that will require extensive collaboration between government and industry. The key is to be on this journey today and not wait until the last minute."

The report contains recommendations for organizations to develop a quantum-readiness roadmap and prepare for future implementation of the post-quantum cryptographic (PQC) standards, which NIST expects to publish in 2024, including steps to effectively prioritize migration efforts. Taking these measures will increase an organization's security posture against potential malicious use of quantum computers.

CISA, NIST, and NSA urge organizations to start preparing for the implementation of post-quantum cryptography by doing the following:

- Establish a Quantum-Readiness Roadmap
- Engage with technology vendors to discuss post-quantum roadmaps.
- Conduct an inventory to identify and understand cryptographic systems and assets.
- Create migration plans that prioritize the most sensitive and critical assets.

By implementing the steps detailed in this CSI, organizations can effectively assess their reliance on cryptographic systems and assets, and prioritize their migration efforts to ensure compatibility with the upcoming PQC standards and meet the goals and timelines in National Security Memorandum (NSM) 10.

15.Algorithm for repelling future quantum data raids proposed by Google

by Jim Nash
https://www.biometricupdate.com/202308/algorithm-for-repelling-future-quantum-data-raids-proposed-by-google

Google says there is "a clear path" to protecting public key cryptography against the moment when quantum computers are used for hacking.

The company is promoting its implementation of the method and has posted it. (There are other ideas.) At stake are all the world's collective databases of biometric and other identity data.

Google bases its conclusion on the creation of the Dilithium algorithm and the standardization of other recent public-key quantum-resilient cryptography.

Much of the cybersecurity community assumes that practical quantum computing, while unavailable now, will arrive before long and quickly tear through standard public-key cryptography like it was wet tissue paper.

Ideally, internet-scale resistance to quantum attacks will arrive before the attacks arrive, says a post by Google.

For that to happen, people will need new security keys after the FIDO Alliance standardizes post-quantum resilient cryptography and browser vendors adopt the standard.

That is going to be a lengthy process, even for a movement that's been around since the early 2000s. Google's implementation combines strong nesting with classical and post-quantum cryptographical schemes. That is, a hybrid of the ECDSA signature algorithm, which Google considers battle tested, and Dilithium.

Company executives say they hope some iteration of their proposal will get baked into the FIDO2 key specification and, of course, win the acceptance of browser companies.

They have invited the community to push their algorithm around in OpenSK, Google's open-source implementation for keys written in Rust supporting FIDO U2F and FIDO2 standards.

16.Debunking The Top 5 Quantum Computing Myths

by Bernard Marr
https://www.forbes.com/sites/bernardmarr/2023/08/23/debunking-the-top-5-quantum-computing-myths/?sh=3f930df21bef

It makes sense that most people don't understand quantum computing. To most of us, quantum physics is a collection of seemingly wild and crazy ideas, such as particles being able to coexist simultaneously in multiple states or exert influence on other particles over infinite distances. There's no surprise that it's enough to get most people scratching their heads.

Understanding the technical mechanics of this kind of thing usually takes a few years of studying at degree level. Luckily, we won't have to have an Einsteinian grasp of the technicalities to benefit from it. But while it promises to lead us into a new era of discovery in fields like astrophysics, drug discovery and material sciences, there are still a few common misconceptions about what it will do and how it will impact society. Here I'll overview the five that I most frequently encounter.

1. **Classical Computers Will Be Replaced by Quantum Computers**

   Quantum computers are not likely to ever replace classical computers (those that translate information into binary bits – ones and zeroes – in order to digitally process it). There are lots of tasks that will simply never require the immense power of quantum computing, which has the potential to perform calculations that would take classical computers billions or even trillions of years in hours or minutes. However, the average computer user will have no need to use quantum computing for purposes of communication, creativity or business tasks. This means classical computers that are far cheaper and easier to produce will be with us for some time yet.

2. **Quantum Computers Are Faster at Every Kind of Job**

   Quantum computers excel at a subset of mathematical problems that are only required for complex tasks. Lots of these involve scientific research – for example, if physicists want to build a simulation to model the behavior of sub-atomic particles, they need a computer capable of operating on quantum principles. They are also great for modeling non-quantum, but still highly complex, systems such as financial markets, meteorological patterns and biological ecosystems.

One particular mathematical challenge they're used for is optimization problems that involve picking an optimum combination from among a large number of variables. This means they will become increasingly useful in machine learning as neural networks become more complex and capable of analyzing larger volumes of data.

However, when it comes to most day-to-day tasks, we use computers for – from word processing to watching videos and playing games – they're unlikely to offer any significant speed increase just yet. Software developers have spent decades optimizing the way these are done on classical computers, whereas quantum developers are just getting started.

3. Quantum Computing Means the End of Encryption

Quantum computing has important implications for encryption – the technology that underpins basically all privacy and data security on the internet.

It won't render it all useless, but encryption protocols – including those widely used to secure data on the internet, such as RSA and ECC - are far more vulnerable to quantum-powered hacking attacks than they are to classical hacking attacks.

This problem has been on the radar for some time, and cryptologists have been busy working on "quantum-safe" encryption protocols.

In the US, the National Institute of Standards and Technology is currently undergoing an evaluation of the threat and potential remedies of post-quantum encryption. In absolute terms, it's right that there are no protocols that we know for sure will never become vulnerable to quantum attacks. The quantum computing power available to us in 20 years will be exponentially greater than what we have now. However, it's thought that investigations into fields such as lattice-based cryptography and cryptography based on multivariate polynomials will result in new protocols that will be safe for some time yet.

4. There's No Practical Use for Quantum Computers Yet

It's still very early days in the evolution of the quantum revolution, but it's certainly a mistake to think that it hasn't started.

Delivery giant DHL uses quantum computers to optimize delivery routes, Goldman Sachs has developed quantum algorithms that are used to complete financial calculations at high speed, pharmaceutical conglomerate Merk uses quantum chemistry to help develop new antibiotics, and a partnership between BMW and Airbus is working applying quantum technology to the problems around creating new and more efficient fuel cells.

New use cases for quantum computing appear by the day, and the market that's today valued at $866 million globally is forecast to expand to $4.3 billion by 2028.

5. Quantum Computing Is Only Viable for Governments and Big Business

While the cost of quantum computers themselves is certainly high, and they need to be kept and operated in highly secure and controlled environments, access to the technology is coming down in price.

Many of the problems that can be solved with quantum computers are relevant to smaller businesses and organizations, such as optimizing supply chains or creating new products more efficiently.

This means that quantum computing providers are already developing and offering services designed to make the technology accessible to these businesses, which make up over 90 percent of the global economy.

IBM, Google and IonQ are just three examples of quantum computing providers that offer access as-a-service to small companies and research groups.

17.Governments Across The Globe Are Looking to Prepare for and Mitigate The Quantum Threat

by Samantha Mabey
https://www.entrust.com/blog/2023/08/governments-across-the-globe-are-looking-to-prepare-for-and-mitigate-the-quantum-threat/

While there's never been doubt about the importance of digital security, over the last few years it seems to have garnered a lot more attention – specifically by governments across the globe. That's no surprise given some of the issues being looked at such as the growth of connected devices and services in the IoT space, for example. But one area that is seeing an increase in calls to action these days is mitigating the threat quantum computers will pose to traditional public key cryptography in use today.

Late last year, we saw an abundance of specific direction coming out of the United States. This direction came in the form of the NSA releasing the CNSA 2.0 Timeline, which outlined the timeline for the migration to post-quantum cryptography (PQC). The timeline spans several years and acknowledges the need to plan and budget for the transition, but it also states that – at least for software and firmware signing – the transition needs to begin immediately. Further, the White House issued not one, but two clear calls to action for government agencies to begin preparing for the quantum threat by designating a lead for collecting cryptographic information systems by December 2022, and then they must have also performed a cryptographic inventory by May 4, 2023.

But attention around the quantum threat and the need to migrate to post-quantum cryptography isn't limited to the United States. This is a global issue, and as such, has garnered global attention. Here are a few examples.

- The General Intelligence and Security Service (AIVD) of the Netherlands very recently released a handbook that advises all organization to start preparing for the quantum threat now, and it also provides some clear steps to begin on that journey.

- The European Union Agency for Cybersecurity (ENISA) produced a report that outlines what organizations can implement now to ensure their data remains secure, including the strategy of choosing a hybrid implementation, which would mix traditional cryptography with quantum-safe cryptography.

- The Federal Office for Information Security (BSI) in Germany published its own guide with the intent of outlining the threat, demystifying PQC, and making recommendations on how to prepare.

- The National Agency for the Security of Information Systems (ANSSI) in France has a position paper. The paper expresses France's views on the quantum threat – including that the threat should be considered today to address the current threat of "harvest now, decrypt later," where sensitive data is being collected by bad actors today, with the intent of decrypting it once a quantum computer is capable.

One thing all the above countries and more (such as Canada, the UK, and Australia) have in common is everyone is awaiting the results of the National Institute of Standards and Technology's (NIST's) competition and the subsequent standards. NIST kicked off a post-quantum cryptography competition, announced the first set of winners in the summer of 2022, and is expected to release draft standards any day now. Although a few European countries have been looking at other algorithms, that's merely to have options on top of what NIST recommends. A recent discussion paper out of the European Policy Centre drives home the importance of a coordinated European action plan, but really this needs to be a global coordination to avoid fractured standards. NIST is seen as the gold standard for independent, open, and transparent competitions, so ideally once NIST comes out with its final recommendations, that will result in international standards and adoption.

18.Google Chrome Adds Support for a Hybrid Post-Quantum Cryptographic Algorithm

by Casey Crane
https://www.thesslstore.com/blog/google-chrome-adds-support-for-a-hybrid-post-quantum-cryptographic-algorithm/

On Aug. 10, the Chromium Project announced in a blog post by Devon O'Brien its adoption of a hybrid cryptographic algorithm (X25519Kyber768) for Chrome and Google Servers. The goal is to help organizations globally secure their data against future quantum computing-based threats while ensuring security against today's cryptographic threats.

In December 2022, the U.S. Congress passed legislation encouraging federal agencies to adopt quantum-resistant cryptography. Some quantum computing (QC) algorithms are already being used by companies like Amazon Web Services (AWS), Cloudflare, and IBM. While widespread adoption of quantum computers will be great when used by well-intentioned people, it also poses a significant threat should that technology fall into the wrong hands.

From an organizational security perspective, Google's move represents the first real opportunity for users to use post quantum cryptography (PQC) for HTTPS. But what does this mean for your business and the security of your customers and users, whose data you're entrusted to protect?

Overview: Google Chrome 116 Adds Support for Its First Public Post Quantum Algorithm

Google is testing new PQC algorithms as part of its multi-year goal of preparing for the PQC future. Starting officially with Chrome version 116, the browser has added support for a quantum-resistant algorithm called X25519Kyber768.

Google explains, the algorithm is a "hybrid mechanism" that "combines the output of two cryptographic algorithms to create the session key used to encrypt the bulk of the TLS connection." The two algorithms used are X25519 (an elliptic curve algorithm already in use) and Kyber-768 (a winner of the NIST PQC competition).

Google ran a test several years ago where they rolled out another quantum computing hybrid algorithm, CECPQ1, to a limited group of Chrome Canary (the experimental version of Chrome) users, but this is the first algorithm rolled out for general use.

PQC Is Now Available for Both Clients and Servers

We've been talking about post-quantum encryption for a while, and this is the first algorithm to be supported by commonly used clients (browsers) and servers.

Alongside Google Chrome's support:

- Google announced that they are also rolling out support for X25519Kyber768 to Google Servers.
- Cloudflare previously announced they had added support for Kyber on "all websites and APIs served through Cloudflare."

Of course, we don't want to overstate what's happened here — this is just one algorithm being supported by one client and a couple of server providers. There are many other steps needed to migrate the internet to post-quantum cryptography (quantum-resistant digital signatures, for example), but this is a very tangible milestone in the journey.

If you want to know more details about quantum cryptography, what the changes are regarding the hybrid algorithm, and why it's a smart move, then keep reading. But first, we want to address how to check what cryptographic security measures you're currently using and how to enable them in Chrome.

.

.

.

19.NTT Research CIS Lab Director Wins Second IACR Test-of-Time Award for Paper on Oblivious Transfer

by Chris Shaw and Stephen Russell

https://www.businesswire.com/news/home/20230817648439/en/NTT-Research-CIS-Lab-Director-Wins-Second-IACR-Test-of-Time-Award-for-Paper-on-Oblivious-Transfer

NTT Research, Inc., a division of NTT, today announced that a paper co-authored by Distinguished Scientist and Director of the Cryptography and Information Security (CIS) Lab **Brent Waters** has won an International Association for Cryptologic Research (IACR) **Test-of-Time (ToT) Award**. Waters and co-authors Chris Peikert and Vinod Vaikuntanathan delivered their paper, "A Framework for Efficient and Composable Oblivious Transfer," at the Crypto 2008 conference. The IACR gives Test-of-Time Awards annually to papers that were delivered 15 years prior at each of the three IACR general conferences (Eurocrypt, Crypto and Asiacrypt). A five-member IACR committee selects the winners based on a consensus view of a paper's impact on the field. In addition, CIS Lab scientists co-authored 14 papers accepted for Crypto 2023. A cryptography researcher with the NTT Social Informatics Laboratories (SIL) co-authored another paper for this year's conference, being held August 19-24 in Santa Barbara.

The Test-of-Time Award-winning paper co-authored by Waters introduced a "dual-mode" cryptosystem framework for Oblivious Transfer protocols using a variety of assumptions. Their framework facilitated the realization of "universal composability," a general-purpose model for cryptographic analysis. This was instrumental in strengthening Oblivious Transfer protocols, which are building blocks for secure Multi-Party Computation (MPC). A powerful cryptographic tool, MPC, allows for parties to calculate outputs without sharing individual inputs. The Crypto 2008 paper was also an early adopter of lattice-based Learning with Errors (LWE), which to date has proven to be quantum resistant. Waters, who is also a Professor of Computer Science at the University of Texas, Austin, won a Test-of-Time Award in 2020 for a paper on Attribute-Based Encryption presented at the Eurocrypt 2005 conference. Like other papers so honored, the paper on Oblivious Transfer had a breakthrough effect, with an enduring influence.

"Around 2008, universal composability was generally regarded by the theory community as the 'gold standard' for security that we aspired to, but it required heavy cryptographic machinery, complex security proofs – and it was decades away from being practically feasible and relevant," CIS Lab Senior Scientist Hoeteck Wee said. "This work changed all of that by providing a solution that is simple, elegant and very efficient. It paved the way towards the adoption of universal composability in practical MPC research efforts today. And it laid the foundations for a unified algebraic framework towards number-theoretic and lattice-based approaches for constructing cryptographic schemes."

One of the paper's key technical contributions was a simple and novel abstraction called a dual-mode cryptosystem. It was implemented by taking a unified view of several cryptosystems in the literature that had what the authors called "message lossy" public keys, whose defining property was that a ciphertext produced under such a key carried no information about the encrypted message. "Today the notion of 'message lossy' keys introduced in the 2008 paper comes up in discussions among groups of junior researchers working on very different topics," Wee said. "This concept has become so in-grained in our cryptographic mind-set and toolkit that we all take it for granted as something everyone knows and understands."

For the Crypto 2023 program, ten scientists from the CIS Lab and NTT SIL, including two post-doctoral fellows, co-authored 15 papers spanning a range of categories. These cryptographers delivered two or more papers that fell under the program headings of Secret Sharing, Functional Encryption, Obfuscation, MPC – Emerging Models and MPC Round Efficiency. The other NTT papers fell into these categories: Quantum Cryptography, Consensus, Emerging Paradigms, ZK (Zero Knowledge) Used on DL (Discrete Log) and Quantum Protocols. The CIS Lab co-authors of these papers were Elette Boyle, Arka Rai Choudhuri (post-doc), Sanjam Garg, Vipul Goyal, Ilan Komargodski, Chen-Da Liu-Zhang (post-doc), Brent Waters, Daniel Wichs and Mark Zhandry. Junichi Tomida represented NTT SIL.

The Crypto 2023 program committee, which accepted 124 papers overall, invited Hugo Krawczyk of the Algorand Foundation to deliver the IACR Distinguished Lecture. Scott Aaronson, of the University of Texas, Austin, and OpenAI, was invited to give a talk on Neurocryptography. The proceedings of the IACR's flagship conferences, which draw the world's leading cryptographers, are published by Springer in its Lecture Notes in Computer Science series.

20.Taiwan needs early quantum-safe migration to stay in the game

by Jennifer Lin and Sophia Yang

https://www.taiwannews.com.tw/en/news/4971615

With more countries developing post-quantum cryptography (PQC), it has become necessary to make the transition to post-quantum encryption as soon as possible, and Taiwan is no exception as the country has seen a sharp increase in cyberattacks.

Dr. Yang Bo-Yin, research fellow at the Institute of Information Science, Academic Sinica, recently spoke with Taiwan News, and suggested the government form a consensus about the post-quantum transition and fund talent acquisition that can properly address the threats associated with quantum computers, which will easily be able to break cryptography currently used to protect our most sensitive data.

Sensitive data exposure

Looking at the future of cryptography, Yang said that in 30 years the words “post quantum” might no longer be in use as any cryptosystem that fails to withstand quantum decryption will all have been phased out.

When asked about when quantum computers could start breaking existing public-key cryptography, Yang said it’s still under debate. “It could be five years, ten years, or longer,” Yang replied.

He said there are tons of valuable and sensitive data that needs to be secured long-term, from government agencies, banks, to medical institutions. “Migrating from a non-quantum resistant public-key scheme to quantum-resistant public-key cryptography algorithms, will take at least around five to ten years, during this time institutions are vulnerable to cyberattacks that leverage quantum computers,” Yang added.

While cryptography sounds like something detached from everyday life, in information security applications, such as in full storage encryption in PC and handheld hardware, financial IC cards, and end-to-end encryption in SMS software, which everyone uses whether they know it or not, people are actually surrounded by cryptography applications today.

Yang said some national-level players are identifying and collecting sensitive encrypted data that they can crack once quantum computers are available.

To improve cybersecurity, the U.S. issued a National Security Memorandum in 2022 requesting all federal agencies and their contractors to switch to quantum decryption-resistant technology as possible by 2035. "Many thought this was too slow, but to make this happen earlier would require a lot more talent and resources than is available," he put.

How PQC started

“Post-quantum cryptographic algorithms didn’t just appear today; they were first introduced in 1978, when Robert McEliece developed such an asymmetric encryption algorithm. After Shor showed classical public-key cryptography - RSA and Elliptic Curves Cryptography - to be crackable using quantum technology in 1994, some people realized the need for new cryptography.”

In 2003, the term “post-quantum cryptography” was coined to differentiate quantum-resistant cryptosystems from conventional ones. It is not a brand-new discipline, nor does it only deal with brand-new cryptosystems. It has only seen increased attention in the last 7 to 8 years.

In 2006, a group of researchers of post-quantum cryptography got together and held the first PQCrypto – an annual conference on post-quantum cryptography. It is not the top-rated or most famous conference but still attracts plenty of academic and industry interest.

“Yang talked about the progress of IBM in quantum computing, which has been one of the frontrunners. IBM scientists simulated quantum bits with seven hydrogen atoms in a large molecule 25 years ago. They were able to run Shor’s quantum integer-factoring algorithm to factor the number 15 as three times five. The number of qubits has only increased into the hundreds today. This does not sound like a big quantitative advance but present-day qubits are scalable as in trapped atoms or superconducting elements, so qualitatively there has been a big leap forward.

Yang said he has researched quantum-safe cryptography for 20 years. He said part of the reason for working on quantum-safe cryptography is simply the beauty of the research and intellectual curiosity, which is partly a religious issue, sort of like why some people climb mountains – because the mountain is there.”

Mindset needs to change

Yang believes that both the theory and the practice of post-quantum cryptography need to be studied, and Taiwan’s strength in semiconductor manufacturing should be a key strength which makes it possible for Taiwan to develop a strong industry presence in PQC, a playground that Taiwan cannot afford to be absent from.

Yang made three suggestions for the government. The first is to build consensus among stakeholders and the public, second is that the government should take a proactive role by not only clearing legal hurdles but also making software safe, efficient, and free to all parties, and third is to attract overseas scientists and engineers to work in Taiwan by providing generous financial incentives.

“We have to compete with Silicon Valley firms in acquiring quantum-safe cybersecurity talent and the compensation offered by the public sector should be generous enough to lure them to work in Taiwan,” said Yang. He used salaries at Google, IBM, and Amazon as examples, saying experienced R&D personnel are usually paid much more than their peers in Taiwan. Yang said higher salaries need to be offered across Taiwan’s information security sector, among others.

Yang said spending on talent and high-performance computing (HPC) needed for post-quantum cryptography research is much less costly compared to spending in the biomedicine, biochemical, and pharmaceutical sectors. “Fourteen years ago, I spent NT$1 million on a high-performance computing server and the machine was just retired,“ Yang said. “The sunken cost for post-quantum cryptography is not as high as for pharmaceuticals, where a single tube of reagents could run tens of thousands New Taiwan Dollars, but you also can’t expect to see returns in a short period of time,” he added.

“Another problem is that everyone inevitably treats security as a cost. Of course, it takes time and money to achieve security, but we have to make everyone aware that spending on security is both cost effective and also a “must,” Yang said. “You will endure ever rising costs from ever increasing security issues if you fail to offer a safe cryptography environment from the beginning.”

Actions needed

Yang advised government agencies, like in the U.S., to start demanding that in seven to 10 years contractors adopt quantum decryption-resistant technologies as part of a push in the transition to post-quantum cryptography in private sectors. A contractor will not switch to post-quantum unless pushed, if for nothing else, because the supply of programmers who could do a post-quantum system is smaller.

The government should also be making it more worthwhile for businesses adopting post-quantum technologies, because losses from being hacked would be so much more than what you would have paid out in transitioning to PQC. This is also why the government should be making much of the software safe, efficient, and free to all parties.”

Yang encouraged public and private sector information security officers to make an action plan with a schedule to phase out old, non-quantum-resistant or insecure cryptosystems and replace them with secure and post-quantum alternatives at a pace commensurate with their risks. To lower the cost incurred in transitioning to post-quantum cryptography, the government should spend resources on producing efficient and formally verified free post-quantum libraries for all to use and indemnify their use.

As for who to emulate in post-quantum cryptography, Asian countries are not very proactive in forming their own PQC ecosystems. Only in South Korea do we see that research teams are now competing to develop their own quantum safe cryptography standard. China also runs its own competition, although it will likely choose a state-backed national standard rather than one developed by any Chinese university or private sector company.

Yang said the Post-Quantum Cryptography Standardization Conference held by the National Institute of Standards and Technology (NIST) is designed to standardize one or more quantum-resistant public-key cryptographic algorithms, which usually end up as a global standard. That explains why the NIST competition is the most anticipated event among public-key cryptography specialists around the world.

Yang shared his own experience participating in the NIST competition last year. His team's "Rainbow" multivariate signature scheme, which was based on the Unbalanced Oil and Vinegar (UOV) scheme, made it to the finals, but was eliminated after being elegantly cracked by young Belgium scholar Ward Beullens.

Yang did not view the defeat a complete waste of time. He said any new cryptography algorithm after being proposed will be parametrized for security and practicality, then enough people need to be convinced to use it practically. This was the case for both UOV and Rainbow, which shared most properties and implementation components.

It was natural to ask him at this point why UOV wasn't proposed instead. "Rainbow had made some efficiency-related modifications, the decision to do that being proven conclusively wrong by Beullens. However, UOV is still the front-runner in this round," he replied.

Stay abreast, stay safe

Yang said he preferred not to view quantum-safe crypto as an "advanced deployment," but rather a necessary chore because everyone else is moving forward. "For each bet you make investing in quantum safe cryptography, there is always a risk that this could fail, but if you make no attempt, you are destined to lose the game," Yang said.

Yang called on the public and private sectors in Taiwan to assess their encryption systems and switch to safer ones. Aside from Elliptic-curve cryptography (ECC) and Rivest–Shamir–Adleman (RSA), outdated algorithms like SHA-1 (Secure Hash Algorithm 1), MD5 (Message-Digest Algorithm) are still in use in many places, and Yang called for them to be phased out as soon as possible.

"Taiwan is already behind; we have to leverage our strengths in hardware to stay abreast of the post-quantum transition," Yang concluded.

21.Google Chrome to shield encryption keys from promised quantum computers

by Thomas Claburn
https://www.theregister.com/2023/08/12/google_chrome_kem/

Google has started deploying a hybrid key encapsulation mechanism (KEM) to protect the sharing of symmetric encryption secrets during the establishment of secure TLS network connections.

Devon O'Brien, technical program manager for Chrome security, explained on Thursday that starting in Chrome 116 – due August 15 – Google's browser will include support for X25519Kyber768, an alphanumeric salad that desperately needs a catchy name.

The unwieldy term is a concatenation of X25519, an elliptic curve algorithm that's currently used in the key agreement process for establishing a secure TLS connection, and Kyber-768, a quantum-resistant KEM that last year won NIST's blessing for post-quantum cryptography.

A KEM is a way to establish a shared secret value between two people so they can communicate confidentiality using symmetric key encryption. It's a precursor ritual to secure information exchange over a network. Unless you're a cryptographer or just love math, you're probably fine not knowing the technical details.

Waiting for that fusion-powered quantum computer on Mars

Google is deploying a hybrid version of these two algorithms in Chrome so the web goliath, users of its technology, and other network providers like Cloudflare, can test quantum-resistant algorithms while maintaining current protections.

The Chocolate Factory is doing so because some day, many very bright people believe, quantum computers will be able to break at least some legacy encryption schemes. That belief is what motivated US technical agency NIST in 2016 to call for future-proof encryption algorithms.

Quantum computers, though much discussed, have yet to demonstrate much practical value due to the need for extensive error correction and many times more qubits.

Google in 2019 said it had conducted an experiment that demonstrated quantum supremacy – the idea that a quantum computer could outperform a classical one. But IBM researchers at the time said the same experiment “can be performed on a classical system in 2.5 days and with far greater fidelity.” So it was not much of a win for quantum boosters.

In June this year, however, IBM researchers published a study in Nature that claimed a 127-qubit processor set loose on a particular physics problem can, with sufficient error mitigation, outperform a classical computer. If confirmed by other researchers, the results suggest quantum computers have a path toward relevancy.

Key issue

“It’s believed that quantum computers that can break modern classical cryptography won't arrive for 5, 10, possibly even 50 years from now, so why is it important to start protecting traffic today?" said O’Brien.

“The answer is that certain uses of cryptography are vulnerable to a type of attack called Harvest Now, Decrypt Later, in which data is collected and stored today and later decrypted once cryptanalysis improves.”

O'Brien says that while symmetric encryption algorithms used to defend data traveling on networks are considered safe from quantum cryptanalysis, the way the keys get negotiated is not. By adding support for a hybrid KEM, Chrome should provide a stronger defense against future quantum attacks.

Google's early deployment of the technology also has practical value to network admins because the new hybrid KEM scheme adds more than a kilobyte of extra data to the TLS ClientHello message. When the internet giant conducted a similar experiment with CECPQ2, some TLS middleboxes couldn't handle the traffic because they had a hardcoded limit on message size.

“I think this is a nice development,” said Matthew Green, a cryptography professor at Johns Hopkins University, in an email to *The Register*.

“Quantum computers are probably at least 15 years away, if not more. But in principle any encrypted messages sent today could be stored until those computers are eventually built.”

“By adding post-quantum encryption to today’s connections, that threat is eliminated. Plus this gives us a very good opportunity to test out some of these new encryption systems long before they’re really needed.”

Rebecca Krauthamer, co-founder and chief product officer at QuSecure, told *The Register* in an email that while this technology sounds futuristic, it's useful and necessary today for two reasons.

“First, data is being intercepted today for later decryption in what is referred to as a harvest now decrypt later attack,” she said.

“There are many forms of data shared via browser-based communications that are valuable now, and will continue to be valuable into the future, including private email communications, electronic health records, bank account information, and more.”

Krauthamer said data that needs to be safeguarded in the future should be protected with quantum resilient cryptography today. She also pointed out that President Biden last year signed H.R.7535, The Quantum Computing Cybersecurity Preparedness Act, which requires US government agencies to begin moving toward quantum resilient cryptography.

“Google is making a fantastic step toward enabling users to protect their communications,” she said.

“At QuSecure we are working from a parallel angle allowing organizations and governments to enable quantum resilient encryption for their own data and that of their users. We will sometimes hear our clients asking if it's already too late to deploy this kind of technology to protect their data if some of it has already been harvested. The answer is absolutely not, but we cannot wait any longer.”

Second, said Krauthamer, the arrival of capable quantum computers should not be thought of as a specific, looming date, but as something that will arrive without warning.

“There was no press release when the team at Bletchley Park cracked the Enigma code, either,” she said.

“Revealing these developments would have shifted the balance of power. If you've created an incredibly powerful tool, you don't show your hand, whether you're working for good or bad. This principle is going to apply to whoever achieves a cryptographically relevant quantum computer. It's a game where keeping the upper hand means keeping secrets.”

“This means that we can’t know when it will come online, but it will likely happen without our knowledge, and it’s imperative we deploy this defensive technology today to not be caught flat footed.”

22.Quantum in China: Insights into China's Advancement in Quantum Technologies

by Matt Swayne
https://thequantuminsider.com/2023/08/10/quantum-in-china-insights-into-chinas-advancement-in-quantum-technologies/

In a recent episode of The China Power Podcast, Dr. Edward Parker, a physical scientist at the RAND Corporation, discussed China's advancements in quantum technologies. Quantum technology encompasses quantum computing, quantum communications and quantum sensing.

Dr. Parker provided insights into China's ambitions and progress in these areas during the interview.

Understanding Quantum Technology

Quantum technology relies on the behaviors of atomic and subatomic particles to collect, process, or transmit information. It encompasses three main applications: quantum computing, quantum communications, and quantum sensing.

Dr. Parker explained these applications as follows:

- **Quantum Computing:** Quantum computers operate on principles different from traditional computers and have the potential to solve certain math problems much faster. While quantum computers are not yet fully developed, their applications include drug discovery, scientific modeling, logistics and artificial intelligence.

- **Quantum Communications:** Quantum communications allow ultra-secure transmission of information that is difficult to intercept or hack. Commercial products for secure quantum communication have been available since 2007, with China being a more prominent user in this field.

- **Quantum Sensing:** Quantum sensors push the limits of sensitivity allowed by the laws of physics. They have various potential applications, such as accelerometers, electric field sensors, magnetic field sensors, gravity sensors, and atomic clocks. While atomic clocks are already widely used, many other quantum sensors are still in the laboratory or experimental stage.

China's Advancements in Quantum Technologies

China has made notable progress in the field of quantum technologies, particularly in quantum communications. Dr. Parker highlighted key milestones:

1. **Quantum Communications:** China has launched two satellites capable of performing quantum key distribution, a secure form of communication. These satellites establish secure communication channels between ground stations and enable encryption that is difficult to hack. China has also laid down an extensive fiber optic network for quantum key distribution, connecting major cities along the east coast of the country.

2. **Quantum Computing:** China has made advancements in superconducting qubits, a mature approach in quantum computing. While China's portfolio of advanced quantum technologies is narrower than the United States, they have demonstrated comparable capabilities in specific areas.

Comparing China's Quantum Advancements

Dr. Parker emphasized that comparing China's progress in quantum technologies with that of the United States is nuanced and complex.

The United States appears more advanced in quantum computing and quantum sensing, while China has made strides in quantum communications. However, Dr. Parker acknowledged the difficulty in drawing definitive conclusions due to limited transparency regarding investment figures and conflicting estimates.

Implications for US-China Competition

Quantum technologies have both economic and national security implications.

The primary concern for the United States in quantum technology is the risk to encryption posed by quantum computers capable of deploying Shor's algorithm. It is a technical risk rather than specific concern about China. The US government has initiated steps to upgrade communication systems and develop countermeasures.

Export Controls on Quantum Technologies

The question of imposing export controls on quantum technologies, similar to those implemented on advanced semiconductors, arises. Dr. Parker cautions against broad export controls on quantum computing and communications, as these technologies are still in an early stage. However, targeted export controls on specific organizations or sensors that provide military operational advantages may be appropriate.

The Significance of Quantum Technology for the US

Quantifying the significance of quantum technology for US competition with China is challenging. Dr. Parker cited varying expert opinions.

Quantum technology has the potential for significant economic value and national security implications, but the precise applications are uncertain. Encryption risk from quantum computers remains a concern. Artificial intelligence (AI) is viewed as having a higher probability of transformative impact, while quantum technology's impact remains uncertain.

Bottom Line: Continuing R&D is Crucial

Quantum technology holds significant potential for economic and national security advancements. China has made notable progress in quantum communications, while the United States remains prominent in quantum computing and sensing. The United States has concerns about the risk to encryption and takes steps to upgrade communication systems. While the importance of quantum technology for US-China competition is uncertain, it is crucial to continue research and development to explore potential applications and address security risks

23.Scientists Propose Naming 2025 'International Year of Quantum Science and

Technology'

by Matt Swayne
https://thequantuminsider.com/2023/08/09/scientists-propose-naming-2025-international-year-of-quantum-science-and-technology/

An alliance of leading scientific bodies and academies from around the world is presenting a resolution to recognize quantum science and technology to the 2023 General Conference of UNESCO and the 2023 General Assembly of the United Nations.

The resolution seeks to declare 2025 as the International Year of Quantum Science and Technology, celebrating the transformative impact of quantum science on technology, culture, and our comprehension of the natural world.

The selection of 2025 for this significant international event commemorates a century since the inception of quantum mechanics, according to the scientists.

Over the past hundred years, quantum science and technology have emerged as central pillars in various scientific and engineering disciplines, spanning physics, chemistry, material science, biology and information science. It has unlocked the secrets behind the sun's brilliance, the workings of magnets, chemical bonding between atoms, and the formation of galaxies in the universe. Moreover, it has paved the way for groundbreaking technological advancements such as transistors powering our electronics, lasers fueling global telecommunications and LEDs revolutionizing lighting efficiency.

Key to Global Challenges

Looking to the future, quantum science and technology are poised to become the paramount interdisciplinary field of the 21st century, significantly impacting pressing global challenges addressed in the UN's 2030 Sustainable Development Goals, according to the website. For example, quantum innovations will play a vital role in addressing issues related to climate, energy, food safety and security and clean water.

By inspiring and nurturing young minds worldwide, the project aims to foster the next generation of quantum pioneers, who will harness quantum science to create a positive impact on humanity. This proposed International Year will offer a unique opportunity for both young and inquisitive individuals of all ages to delve into the ways quantum science underpins our physical world, drives technological breakthroughs, and influences art and culture.

The initiative achieved a major milestone in October 2021 when the International Union of Pure and Applied Physics (IUPAP) endorsed the proposal during its 30th General Assembly. The IUPAP expressed "strong support for the International Year of Quantum Science and Technology goals, encompassing science, education, outreach, and particularly aiming to promote physics education and improve the quality of life for citizens in developing nations."

This global endeavor is part of a broader initiative dedicated to enhancing national capabilities in fundamental sciences and science education.

24.Android 14 takes aim at insecure cryp-

tography in cellular networks

by Timi Cantisano
https://www.xda-developers.com/android-14-2g-network-protection/

For years, Android has been strengthening its security in order to keep users safe. With each new release, Google has introduced features that not only keep users safe from obvious malicious activities but also areas where consumers might not have as much control like cellular network traffic. Because of this, Google is now introducing new protections to Android with “advanced cellular security mitigations” in Android 14 that will protect both consumer and enterprise users.

With wireless companies shifting more of its network to 5G, available resources need to be put to better use, and that means shutting down older 2G networks that are rarely put to use. Most wireless carriers have committed openly to shutting down these networks over the next ten years, so while rare, it is still possible to connect to these 2G networks when other options aren't available. Now as you can imagine, 2G networks aren't as advanced when it comes to security when compared to more modern 4G and 5G networks.

Because 2G networks are less secure, they can be used as attack points, so there are methods that can be used to automatically downgrade a device to this network in order to perform malicious attacks. This can be accomplished because 2G networks lack mutual authentication and can allow for over-the-air interception and decryption of data on that network. With all that said, Google has been working on making Android devices safer and has shared through its *Google Security Blog*, new features that it will introduce that allows users to disable 2G connections at the modem level, creating protections against these kinds of attacks. While it was first introduced with Android 12, it can now be implemented on all devices, so long as the manufacturer enables it and the device supports HAL 1.6+.

With Android 14, this type of protection will be expanded, giving enterprise users the ability to manage devices and restrict a device's ability to downgrade its connection to 2G, keeping it safe from attacks. This will be especially important for those that travel to "high-risk" locations and will be a critical feature that can protect a user and a device's data. In addition, administrators will still be able to keep tabs on all managed devices, with audit logging that can track over 80 events and over 200 different management controls. In addition to the above, Android 14 will also attempt to protect circuit-switched voice and SMS traffic.

This is typically handled by cellular networks, and it is up to each company whether to leave this kind of information encrypted or not. Android 14 will introduce an option to disable support for null-ciphered connections. This will provide protection against unencrypted networks, and Google expects that this type of feature will be more widely adopted by companies over the next few years. As in the past, Google will also continue to work with cellular companies and standards bodies like the GSMA Fraud and Security Group, 3rd Generation Partnership Project, and others, to improve the security of networks.

Although new features and cosmetic enhancements are always welcome, these types of security features are also a critical part of any new Android release. Android 14 is expected to release later this year, alongside new products from Google that will take advantage of the aforementioned enhancements. While the brand has been fairly quiet about what's to come, we've seen and heard rumors of the upcoming Pixel 8 and Pixel 8 Pro. Regardless of what makes an appearance, it's good to know that new security features will be made available to all compatible Android devices.

25.SandboxAQ Introduces Open-Source Quantum Encryption Library for Software Developers

by Naomi Cooper
https://executivebiz.com/2023/08/sandboxaq-intros-open-source-quantum-encryption-library-for-software-developers/

Quantum software company SandboxAQ has unveiled an open-source encryption library that works to enable software developers to use cryptographic algorithms to create more secure applications.

Sandwich provides tools designed to embed post-quantum cryptography algorithms directly into software applications and swap cryptographic elements without rewriting code, SandboxAQ said Tuesday.

The meta-library works with open-source cryptographic libraries OpenSSL, BoringSSL and libOQS and supports languages C/C++, Rust, Python and Go upon launch.

Sandwich features a unified application programming interface to allow easy integration and streamline modern cryptography management.

SandboxAQ plans to make future additions to the library based on feedback from the open-source communities.

“With Sandwich, we’re empowering developers to experiment with different types of cryptography – including the new post-quantum cryptography algorithms soon to be standardized by NIST – so they can achieve the right balance of security and performance,” said Graham Steel, head of product for SandboxAQ’s security group.

26.China hacked Japan’s sensitive defense networks, officials say

by Ellen Nakashima
https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/

In the fall of 2020, the National Security Agency made an alarming discovery: Chinese military hackers had compromised classified defense networks of the United States’ most important strategic ally in East Asia. Cyberspies from the People’s Liberation Army had wormed their way into Japan’s most sensitive computer systems.

The hackers had deep, persistent access and appeared to be after anything they could get their hands on — plans, capabilities, assessments of military shortcomings, according to three former senior U.S. officials, who were among a dozen current and former U.S. and Japanese officials interviewed, who spoke on the condition of anonymity because of the matter’s sensitivity.

“It was bad — shockingly bad,” recalled one former U.S. military official, who was briefed on the event, which has not been previously reported.

Tokyo has taken steps to strengthen its networks. But they are still deemed not sufficiently secure from Beijing’s prying eyes, which, officials say, could impede greater intelligence-sharing between the Pentagon and Japan’s Defense Ministry.

The 2020 penetration was so disturbing that Gen. Paul Nakasone, the head of the NSA and U.S. Cyber Command, and Matthew Pottinger, who was White House deputy national security adviser at the time, raced to Tokyo. They briefed the defense minister, who was so concerned that he arranged for them to alert the prime minister himself.

Beijing, they told the Japanese officials, had breached Tokyo’s defense networks, making it one of the most damaging hacks in that country’s modern history.

The Japanese were taken aback but indicated they would look into it. Nakasone and Pottinger flew back “thinking they had really made a point,” said one former senior defense official briefed on the matter.

Back in Washington, then-President Donald Trump was busy contesting Joe Biden’s election victory, and administration officials were preparing for a transition. Senior national security officials briefed incoming national security adviser Jake Sullivan during the handoff, but the incoming Biden administration faced a swirl of issues — including how to deal with a major Russian breach of U.S. agency networks discovered during the Trump administration — and some U.S. officials got the sense the Japanese just hoped the issue would fade away.

By early 2021, the Biden administration had settled in, and cybersecurity and defense officials realized the problem had festered. The Chinese were still in Tokyo’s networks.

Since then, under American scrutiny, the Japanese have announced they are ramping up network security, boosting the cybersecurity budget tenfold over the next five years and increasing their military cybersecurity force fourfold to 4,000 people.

The stakes are high.

Beijing, bent on projecting power across the western Pacific — an area it controversially claims as part of a historic maritime dominion, has increased confrontation in the region. It fired ballistic missiles into Japan’s exclusive economic zone last August after then-House Speaker Nancy Pelosi (D-Calif.) visited Taiwan, a self-ruled democracy that China claims. It has embarked on a major nuclear weapons buildup. And it has engaged in dangerous air and naval maneuvers with U.S., Canadian and Australian ships and jets in the Pacific.

China, which already boasts the world’s largest legion of state-sponsored hackers, is expanding its cyber capabilities. Since mid-2021, the U.S. government and Western cybersecurity firms have documented increasing Chinese penetration of critical infrastructure in the United States, Guam and elsewhere in the Asia-Pacific. The targets include communication, transportation and utility systems, Microsoft said in May.

China-based hackers recently compromised the emails of the U.S. commerce secretary, the U.S. ambassador to China and other senior diplomats — even amid an effort by the Biden administration to thaw frosty relations with Beijing.

“Over the years we have been concerned about its espionage program,” said a senior U.S. official. “But China is [also] developing cyberattack capabilities that could be used to disrupt critical services in the

U.S. and key Asian allies and shape decision-making in a crisis or conflict."

In the face of this aggression, Japan has stepped up, moving beyond the traditional "shield and spear" arrangement in which Tokyo focuses on the country's self-defense, while Washington provides capabilities that support regional security, including the nuclear umbrella that protects Japan and South Korea. Japan is developing a counterstrike capability that can reach targets in mainland China. It is buying U.S. Tomahawk cruise missiles. And it is permitting the U.S. Marine Corps to place a new advanced regiment in remote islands southwest of Okinawa, a location that, along with the northernmost islands of the Philippines, allows the U.S. military proximity to Taiwan should a conflict with China erupt.

"Japan and the United States are currently facing the most challenging and complex security environment in recent history," Prime Minister Fumio Kishida said at a news conference with President Biden in Washington in January. He noted Japan's new national security strategy boosting its defense budget and capabilities. "This new policy," he said, "will be beneficial for the deterrence capabilities and response capabilities of the alliance as well."

U.S. Defense Secretary Lloyd Austin has indicated to Tokyo that enhanced data-sharing to enable advanced military operations could be slowed if Japan's networks are not better secured.

"We see tremendous investment and effort from the Japanese in this area," said a senior U.S. defense official. But work remains to be done. "The department feels strongly about the importance of cybersecurity to our ability to conduct combined military operations, which are at the core of the U.S.-Japan alliance."

27.EU Late to the Quantum Party, Report Warns

by Tammy Xu
https://spectrum.ieee.org/post-quantum-cryptography-strategy

Companies and governments need to act quickly to develop a comprehensive strategy for quantum readiness, says a new report by the European Policy Center, a think tank for European Union affairs. Given the current pace of quantum computing research, a quantum computer capable of breaking modern cryptography is estimated to arrive within the nexttwo decades. That's barely enough time for policymakers to plan and implement the technical and logistical actions necessary to be ready for a world with quantum computers, says report author Andrea G. Rodríguez.

Quantum computers could wreak havoc on digital communications by breaking public-key cryptography algorithms, which are used everywhere to deliver digital messages securely. When users browse to a secure website like a bank's, public-key cryptography helps the user and website securely exchange a secret key for encrypting all their communications. A quantum computer could blow that all apart by exposing the secret key, allowing attackers to see all communications and potentially impersonate both the user and the website.

But there are still limits to the types of attacks a quantum computer that can break cryptography—also known as a cryptographically-relevant quantum computer (CRQC)—can do. Just getting your hands on one won't immediately grant you access to all existing digital communications. Each cryptographically protected connection is unique, and a quantum computer would need all its computing resources to break one connection at a time. The process also takes time—a few hours to break public-key cryptography using a quantum computer, down from trillions of years on a conventional computer.

“The average user, they have a bank account, and logging in is protected by cryptography,” said Dustin Moody, who leads efforts to develop new quantum-resistant cryptography standards at the National Institute of Standards and Technology (NIST). “But someone who has a quantum computer, that’s not where they’re going to be [targeting] until quantum computers are really cheap and inexpensive to operate. And we’re nowhere near that point.”

In other words, no one should expect a CRQC to be emptying out bank accounts when they first arrive—not because it can’t, but because a bank account isn’t a worthwhile target. Quantum computers will be expensive to operate, and as a result, attacks by quantum computers will likely be directed at high value targets like countries or important industries. In those domains, targets may already be susceptible to “harvest now, decrypt later” attacks that collect encrypted information now for future decryption using quantum computers.

NIST’s post-quantum cryptography standardization project will publish its completed standards in 2024. Moody said that if all goes according to plan, the transition to new cryptographic standards will be mostly invisible to the average digital communications user. Only organizations that use cryptography in their own code, the report says, would need to locate the places where the existing standards are used and replace it with the new ones.

Finding all the places where cryptography is used in a code base, however, is not a trivial task. Bill Newhouse leads the project at NIST that’s in charge of the migration to post-quantum cryptography—the difficult task of actually getting organizations to adopt the new standards. He says his team is currently working with industry partners to develop tools that will help organizations locate all the points in their workflow where quantum-vulnerable cryptography is used.

“For this project, we’re trying to figure out what organizations—whether it’s government or industry—can do to begin to prepare themselves,” Newhouse says. “The concept is, you need to have an inventory of what cryptographic algorithms you rely on today, to hopefully get some notion of which ones are deemed quantum vulnerable based on their use of public-key encryption.” Once that’s determined, the true scope of the work involved to transition to new standards will be better known.

That’s why it’s important for the EU to take action and create a plan immediately, says Rodríguez, author of the EPC report. The EU has spent comparatively less time than the United States developing technical solutions for postquantum cryptography. Although European researchers have devoted substantial resources toward developing a form of quantum-based cryptography called quantum key distribution, that isn’t very mature yet, the report said. It encourages the EU to allocate more resources to postquantum cryptography and also to testing quantum key distribution. But even when new quantum-resistant technologies are ready, migrating users over to them can take years, Rodríguez said.

Individual EU member states have started picking up the slack. A few countries have made plans for countering future quantum cybersecurity threats or have enacted strategies for doing so. But the report warns that this can create “asymmetries” between countries. That can turn into a security flaw, because an attack on any member of the EU affects the others as well, the report said. Instead, it said, the EU should act quickly and cohesively to implement plans for a quantum future.

“As we noticed, we are already late,” Rodríguez says.

28.A Brief Overview of Quantum Comput-

ing in Spain in 2023

by James Dargan
https://thequantuminsider.com/2023/08/04/a-brief-overview-of-quantum-computing-in-spain-in-2023/

Quantum computing, the revolutionary technology that harnesses the principles of quantum mechanics to process information exponentially faster than classical computers, has emerged as one of the most promising fields of research in recent years. As nations worldwide vie for supremacy in this rapidly evolving industry, Spain has firmly established itself as a notable player in the quantum computing race. With a strong focus on research, significant government support, and a thriving private sector, Spain has positioned itself as a quantum hub in Europe.

Government Position

Spain's commitment to quantum computing is evident through its strategic investments and initiatives supported by the government. The Spanish Ministry of Science and Innovation has been at the forefront of promoting quantum research and development.

An important initiative is Quantum Spain, promoted by the Ministry of Economy through the Secretary of State for Digitization and Artificial Intelligence and financed with the Recovery Funds and founded in 2021. The goal of Quantum Spain is to promote and finance the development of a competitive and comprehensive quantum computing infrastructure in Spain.

Research

Spanish research institutions and universities have made significant strides in advancing quantum technologies. The Barcelona Supercomputing Center (BSC) — QUANTIC — has been actively involved in quantum computing research. In collaboration with IBM, the BSC launched the "IBM Q Hub Spain" in 2021, becoming part of IBM's global quantum network. This partnership allows Spanish researchers and businesses to access IBM's quantum computers and collaborate with the broader quantum community.

The Institute of Photonic Sciences (ICFO) in Barcelona is another vital player in Spain's quantum research landscape. Research at the Institute covers a very broad range of topics, from theoretical quantum physics to applied medical optics. An integral part of the institute's mission is to train new scientists and technologists.

The Spanish government's investment in research is also evident through the creation of quantum labs across the country. The Quantum Information and Computation group at the Universidad Politécnica de Madrid (UPM) is one such example.

Others include the University of Castilla La Mancha (UCLM)—Alarcos Research Group and the University of the Basque Country—Quantum Technologies for Information Science (QUTIS).

Private Sector

The Spanish private sector has actively embraced quantum technologies, fostering partnerships with research institutions and startups. Here is a non-exhaustive list of some of the main players in the country.

One notable company is Qilimanjaro Quantum Tech. Founded in 2018 by José Ignacio Latorre, a professor of Theoretical Physics at the University of Barcelona, Qilimanjaro is working on developing quantum processors based on superconducting qubits. Qilimanjaro Quantum Tech is not alone in its pursuit of quantum applications.

Another to note is aQuantum. Based in Madrid, aQuantum is a research, development, consulting and services firm specializing in quantum software engineering and programming. With expertise in quantum software engineering and programming, aQuantum works in the fields of hybrid classical-quantum computing, software quantum quality, governance and management, quantum software workforce, development tools, and machine learning (ML).

Inspiration-Q helps forward-looking companies in their quantum-ready journey through agile adoption of the future quantum revolution and benefits from the short-term advantages of quantum computing. Based in Madrid, the company provides SaaS solutions for quantum-inspired and quantum algorithms, as well as specialized finance applications.

Moving to Catalonia now, we have LuxQuanta, a spin-off company from the Institute of Photonic Sciences (ICFO) in Barcelona. As well as providing mathematical cryptographic techniques on top of quantum-safe systems and technologies, LuxQuanta strives to integrate Quantum Key Distribution (QKD) systems into existing network infrastructures.

One of the more high-profile companies in Spain, Multiverse Computing hails from the Basque region and provides software to companies in the financial industry as well as other verticals seeking to gain an edge through quantum computing. Among the company's areas of expertise are portfolio optimization, risk analysis and market simulation.

Quantum Mads specializes in examining, both theoretically and practically, the inherent dynamics of complex financial systems, and to create solutions that will disrupt current modelling techniques and allow us to have unique insight that will be valuable to our clients. The company is based in Vitoria-Gasteiz.

Like Multiverse Computing, Quanvia's headquarters are in the Basque region, but it has a presence in Washington D.C., US and Santiago, Chile. Through the integration of quantum computing and artificial intelligence, Quanvia provides innovative quantum products in training, research, and consulting.

Finally, we have Barcelona-based Quside, a startup that provides high-quality components for all connected devices using quantum technologies. The company designs ultrafast, quantum random number generation solutions for mobile, IoT and data centres using their proprietary quantum entropy sources.

Key People

As with any field, choosing the most important individuals is challenging, but we were able to select two individuals whose contributions are driving the country forward in quantum technology.

Spain's quantum industry owes much of its success to the dedicated individuals who have paved the way for advancements in the field. Notably, Enrique Solano, a Professor at the University of the Basque Country (UPV/EHU), has been recognized for his groundbreaking research in quantum computation and quantum simulations. Solano's research group at UPV/EHU collaborates with other institutions to explore the frontiers of quantum technologies.

Another notable individual whose contribution to Spain's quantum journey is significant is Elías Combarro, a co-founder of QSpain and Professor of the Computer Science Department of the University of Oviedo. As well as holding these two positions, Combarro is an Associate collaborator of CERN and its Quantum Technology Initiative and a SheQuantum Board Member. His current projects include working with companies like E.ON and Cambridge Quantum Computing as well as institutions like CTIC and CERN.

Conclusion

Spain's quantum computing industry has rapidly evolved into a force to be reckoned with, thanks to substantial government support, cutting-edge research, and a dynamic private sector. Collaborations between academia and industry have been pivotal in bridging the gap between theoretical concepts and practical applications.

As the quantum industry continues to grow, Spain remains committed to pushing the boundaries of quantum computing and exploring the endless possibilities it offers. With innovative companies, world-class researchers, and a supportive government, Spain is poised to make significant contributions to the global quantum revolution.

29.QuEra Launches New Ways to Access Quantum Computers

by Matt Swayne
https://www.taiwannews.com.tw/en/news/4958467

QuEra Computing, the leader in neutral-atom quantum computers, today announced it now supports new ways of accessing its quantum computers to meet the computing, compliance and security requirements of any customer. Under QuEra's new program, its industry-leading quantum computers can now be leased for on-premise use, accessed via a premium service model, or used on a major public cloud. Dozens of companies are now regularly accessing QuEra's quantum computers through these methods.

QuEra's technology is built on large-scale arrays of neutral atoms. It currently offers users up to 256 qubits on its Aquila-class machines, with plans to scale to much higher numbers. QuEra's designs feature a unique combination of system size, coherence, and an innovative analog quantum processing mode that provides new ways to solve machine learning, optimization and simulation problems. Furthermore, Aquila machines offer the added benefit of its FPQA™ technology, a field-programmable qubit array that provides flexible reconfiguration of its qubit positioning, comparable to designing a new chip layout for each computation. The hardware is complemented by Bloqade™, an open-source software package that assists with expressing and testing problems in this new way.

On-Premise

Organizations that need direct access to QuEra's industry-leading 256-qubit quantum computers and want full control over who uses the system and their access priority can now lease machines for on-premise delivery. QuEra's team of experts works closely with each customer to ensure alignment and integration with existing HPC resources, creating a unified, powerful computing environment. Additionally, QuEra offers ongoing support and assistance in workforce and application development.

Premium Access

Premium Access provides a secure connection to a QuEra machine and includes direct support from QuEra's team of exceptional scientists and engineers. Together, QuEra and Premium Access customers collaborate to solve difficult problems. QuEra also provides industry best practices, personalized support, and tailored training programs to enhance the organization's neutral atom quantum computing skills.

Amazon Braket

Customers can continue to access QuEra's Aquila directly using their Amazon Braket account, a fully managed quantum computing service designed to help speed up scientific research and software development for quantum computing.

``As we ramp up the production capabilities and expand our exceptional team of application-focused scientists, we're thrilled to unlock additional avenues for engaging with our ground-breaking technology." says Alex Keesling, CEO of QuEra, ``The launch of our on-premise and premium access models stems directly from resonant customer demand. This pivotal move is not just a response but an exciting leap forward that opens a realm of new opportunities for our customers and for QuEra."

30.Quantum Safe Migration Center launches to improve cyber resilience in Taiwan

by Sean Scanlan and Jennifer Lin
https://www.taiwannews.com.tw/en/news/4958467

In order to welcome the next digital era and security challenges associated with quantum computing, guests from industry, government, and academia gathered on Tuesday (Aug. 1) for the opening of the Quantum Safe Migration Center (QSMC) initiated by Chelpis Quantum Tech, the first of its kind in Taiwan and Asia.

Chelpis Quantum Tech Founder Ming Chi said **the company is dedicated to post-quantum security** and solving client-related security issues. To strengthen the resilience of Taiwan's information security, the Quantum Safe Migration Center will serve as a bridge connecting government, industry, academic institutions, and international researchers.

Chi expects Taiwan, like other European countries and the U.S., will soon issue a blueprint for post-quantum security, incorporating it into a national security plan.

Quantum Safe Migration Center Director Matthias J. Kannwischer studied quantum cryptography for many years, and it was also his doctoral dissertation subject. Over the years, he has thought about combining academia and industry to effectively apply post-quantum cryptography to various fields.

Kannwischer is excited to see academic research being applied to real-world situations, attracting the attention of companies and government agencies. The center is the first such institution in Taiwan and Asia to offer an encryption system that can repel quantum computer attacks.

Director of the Department of Computer Science and Engineering at National Sun Yat-sen University, Dr. Fan Chuni, said Taiwan has many ways to attract the attention of foreign companies for its strengths in semiconductors and IT hardware, creating an ecosystem that integrates precision cybersecurity, low carbon information security, and information security native into a platform.

Fan said Taiwan's post-quantum cryptography sector is segmented as everyone is doing independent work. If the government can form a "post-quantum national team," it could integrate the country's resources and create talent pipelines to achieve advancements in cybersecurity.

National Chengchi University's Computer Science Department professor Raylin Tso said that the Quantum Safe Migration Center can help Taiwan migrate toward post-quantum security, serving as a platform that integrates resources, expertise, and technologies from various universities, allowing everyone to exist on equal footing. Tso said the school expects to have long-term cooperation with the center.

Academia Sinica Institute of Information Science research fellow Yang Bo-yin said Taiwan should provide incentives and attractive salaries to lure highly skilled talent. He said this expense is difficult for the private sector to cover, so the public sector should take the lead.

Yang said that compared with the R&D investment in biomedicine, biochemistry, and pharmaceuticals, the relevant expenditure on post-quantum cryptography is more cost-effective. And although the benefits cannot be seen immediately, it is a necessary investment.

Academia Sinica Research Center for Information Technology Innovation assistant research fellow Tung Chou said government agencies and companies should sort out which data will remain critical as time goes by, say 20 years from now, and transition it to a new encryption system first. Without being protected by the post-quantum technology, this data would become vulnerable to cyberattacks.

The center has the backing of notable organizations or interest groups dedicated to fortifying information security, including the Digital Taiwan Roundtable (DTR), the Institute for Information Industry (III), and the Industrial Technology Research Institute (ITRI) among others.

Quantum Safe Migration Center partners include Academia Sinica, National Taiwan University, National Yang Ming Chiao Tung University, National Sun Yat-Sen University, as well as other academic institutions. In order for Taiwan to transition as soon as possible to a post-quantum cryptography system, the center is also cooperating with several information security experts, accessing their years of experience, relevant insights on quantum security and post-quantum cryptography, and lessons learned through industry-university cooperation.

The center plans on publishing at least one article every quarter, as well as books or guidelines. In the future, the center will set up various working groups to invite foreign scholars and experts to collaborate with their peers in Taiwan through various activities.