Crypto News

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

August 01, 2023

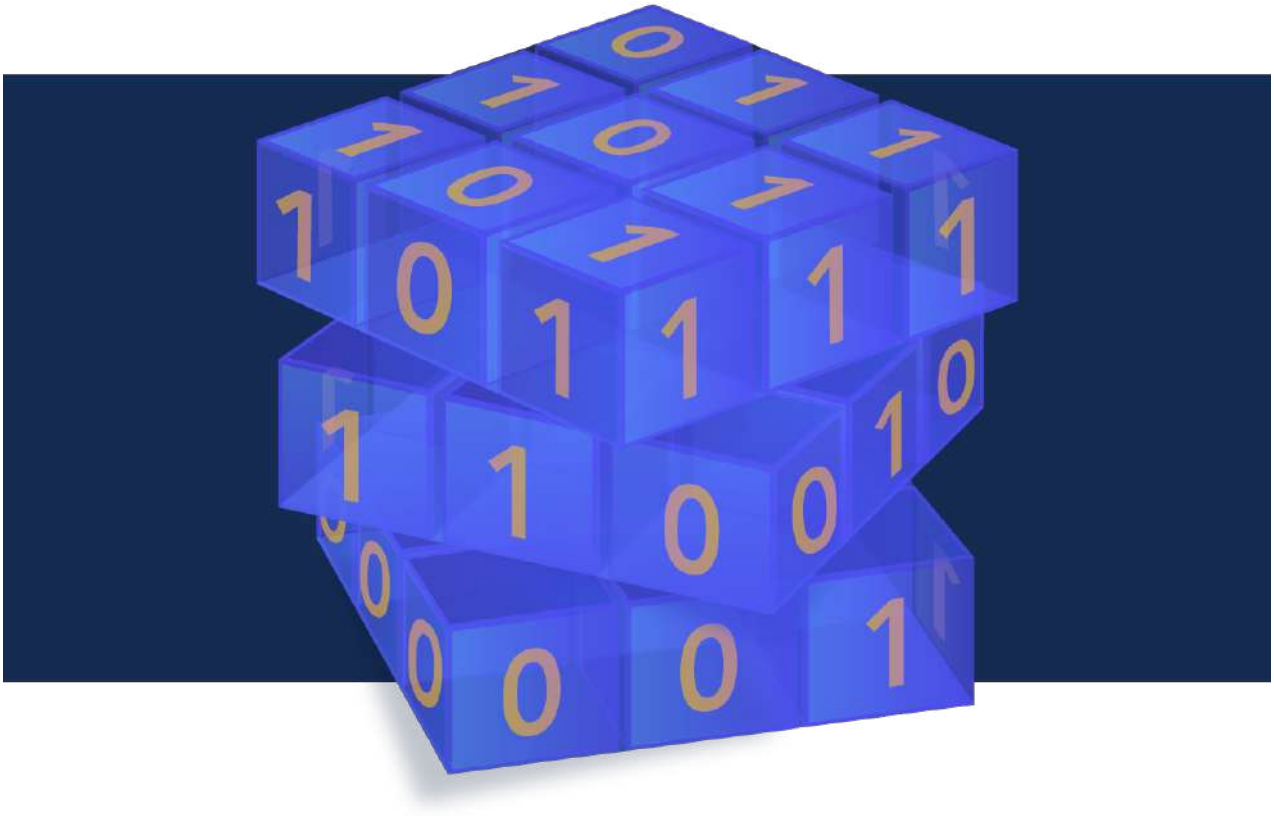

TABLE OF CONTENTS

1.QUANTUM COMPUTERS AND ASYMMETRIC ENCRYPTION: A BATTLE FOR DIGITAL SECURITY 5

2.WORLD'S FIRST ROOM-TEMPERATURE SUPERCONDUCTOR SYNTHESIZED, COULD IMPACT DEVELOPMENT OF QUANTUM COMPUTING AND QUBITS 6

3.U.S. HUNTS CHINESE MALWARE THAT COULD DISRUPT AMERICAN MILITARY OPERATIONS 8

4.CRYPTOGRAPHY MAY OFFER A SOLUTION TO THE MASSIVE AI-LABELING PROBLEM 12

5.BTQ TECHNOLOGIES CORP.'S POST-QUANTUM CRYPTOGRAPHY SCHEME PREON SELECTED BY NIST 14

6.A BRIEF OVERVIEW OF QUANTUM COMPUTING IN SOUTH KOREA IN 2023 15

7.RUSSIAN SCIENTISTS PRESENT 16-QUBIT QUANTUM COMPUTER 18

8.CHINESE SCIENTISTS SAY METROPOLITAN QUANTUM TELEPORTATION REACHES HERTZ RATE 19

9.RESEARCHERS FIND 'BACKDOOR' IN ENCRYPTED POLICE AND MILITARY RADIOS 20

10.POST-QUANTUM CRYPTOGRAPHY: A DECADE OF REVOLUTIONIZING INTERNET SECURITY 22

11.EMERGING SYNERGIES: LEVERAGING AI TO BOLSTER POST-QUANTUM CRYPTOGRAPHIC SECURITY 23

12.PREPARE FOR QUANTUM TO FUNDAMENTALLY CHANGE PKI EFFECTIVENESS 25

13.TII CONTRIBUTES TO POST-QUANTUM CRYPTOGRAPHIC STANDARDIZATION VIA NIST DIGITAL SIGNATURE SCHEMES 27

14.QUANTUM CRYPTOGRAPHY: THE FUTURE OF SECURE DIGITAL PAYMENTS 28

15.CONTROLLING QUANTUM RANDOMNESS FROM THE VACUUM 31

16.QUANTUM TECHNOLOGY — ADVANCING APPLICATIONS IN SPACE 32

17.HARDWARE SECURITY ENTERING QUANTUM COMPUTING ERA 33

18.WHITE HOUSE PUBLISHES NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN 34

19.JAPANESE BANKING GIANT MAKES STRATEGIC QUANTUM INVESTMENT 36

20.INTERNET ENGINEERING TASK FORCE STANDARDISES QUANTUM-SAFE VPN PROTOCOL CREATED BY POST-QUANTUM 37

21.CHINESE HACKERS FORGED AUTHENTICATION TOKENS TO BREACH GOVERNMENT EMAILS 38

22.PREPARING BUSINESSES' DIGITAL TRUST FOR A POST-QUANTUM WORLD 40

23.UNBREAKABLE COMMUNICATIONS USING THE POWER OF QUANTUM CRYPTOGRAPHY 41

24.CYBERCRIMINALS CAN BREAK VOICE AUTHENTICATION WITH 99% SUCCESS RATE 43

25.VODAFONE IS PREPARING FOR QUANTUM ATTACKS ON SMARTPHONES **44**

26.WHY CYBER PROS ARE NERVOUS ABOUT QUANTUM COMPUTING Q-DAY **46**

27.QUANTUM CRYPTOGRAPHY CHALLENGES AND OPPORTUNITIES FOR FEDERAL AGENCIES **48**

28.PROTECTING CONNECTED DEVICES WITH QUANTUM-GENERATED CRYPTOGRAPHIC KEYS **50**

Editorial

With the emergence and use of deep fake videos and AI by larger portions of the population, there is a need to understand the origin of the media that's being generated by these technologies. Cue provenance information. Many companies have been working for years to figure out new and innovative ways to mark media as being AI generated with varying levels of success and progress. A new solution created by the likes of Intel and Microsoft amongst a host of other companies as part of a non-profit organization is on the horizon based on cryptography called C2PA. Think of C2PA as a "nutrition label" for content that shows who or what created it. If you're interested in learning more, scroll down to article 4. I know I'm intrigued!

If you've been following us for a while, you likely noticed our groups focus on quantum cryptography and QKD. So besides protecting data on the internet from bad actors with malicious intent in a post-quantum world, what else can it do? Well, it turns out it's a whole host of things! Make your way to articles 14 and 23 to learn how the digital payments industry and connected devices will benefit. Don't miss the other interesting and thought-provoking articles in this issue of Crypto News! Happy reading!

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

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

1.Quantum computers and asymmetric encryption: A battle for digital security

https://www.cio.com/article/644614/quantum-computers-and-asymmetric-encryption-a-battle-for-digital-security.html

Quantum computing poses a threat to traditional cryptography, but IT leaders are by no means powerless to respond. Identifying and preparing for future risks is core to enterprise cyber-resilience. But it's not something that CIOs need to manage alone. Technology vendors can provide insights and intelligence to help organisations identify emerging threats.

HP is a case in point. With cyber security products and services, and the research of the HP Security Lab at HP Labs, it provides IT decision makers with leading-edge technology and services to help keep ahead of threats.

Just one of the many threats currently on its radar is the potential risk that quantum computing presents to cryptography. In particular, the threat is to a type of cryptography called asymmetric cryptography which today's IT systems rely on massively for the security of data encryption solutions as well as digital signature applications. Many security technologies are at risk including TLS, IPsec, X.509, SSH, and most authentication protocols.

Any potential weakness in cryptography is a global threat. Tommy Charles, chief cryptographer at the HP Security Lab, says: "Losing asymmetric cryptography is analogous to a zero-day attack with the power to break almost every element of the enterprise tech stack, from user authentication and code signing, to encrypted storage and secure network communications. The potential scale of the impact is unlike anything we have seen to date."

Today's asymmetric cryptography uses one-way functions to secure data via a public key. The mathematical problems underpinning one-way functions make it practically impossible to reverse the process without access to the private key.

Quantum computing threatens to fundamentally undermine this approach by taking advantage of how subatomic particles behave. What's more, algorithms designed to run on quantum computers ensure probabilities accumulate while they run, making it possible to crack even the most challenging of mathematical puzzles. And while today's quantum computers are only making a start, it is expected that the technology will mature and give them the speed and power of calculation to threaten cryptography.

"As quantum computing progresses, cryptographic inversion becomes easier. Threat actors will be able to crunch numbers in huge volumes while also enabling the probabilities for solving the underlying mathematical problem to stack up," says Thalia Laing, cryptographer and security researcher at the HP Security Lab.

How likely is it that this threat will materialise? According **to a survey of quantum experts** by the Global Risk Institute, 50% of respondents believe there's more than a 30% chance of a cryptographically relevant quantum computer being invented by 2032. For Charles, this is a risk no business should take: "no matter how you look at it, there's a significant chance that the cryptography your business relies on most is going to be broken. Businesses have an imperative to act," he says.

Fortunately, progress is already being made in the area of new, quantum-safe encryption standards. The

US' National Institute of Standards and Technology (NIST)has led an international collaboration which recently **selected four quantum-resistant algorithms** that are able to run on standard, binary computers.

Three of these solve the quantum dilemma through "structured lattices", which use many more mathematical equations than in legacy asymmetric cryptography which relied on the hard "factorisation" problem. The new approach adds "noise" to encryptions through deliberate errors. With structured lattices, recovering values from encrypted text is a near-impossible challenge, even using quantum computing.

However, the move to quantum-safe cryptography will take time and involve considerable effort. Laing says: "It's likely that cryptographic algorithms in use today will be replaced by a broader suite of quantum-safe alternatives. This will help businesses provide protection for their various use cases with best-fit solutions, while also building resilience by having some fallback options. And with the use of new algorithms, a vulnerability may yet be discovered in how they are used. As such, it is likely that legacy and new algorithms will coexist for a while in a hybrid approach until quantum-safe technology matures."

HP can already advise businesses on how to plan for a quantum-safe future. For IT leaders who want to understand the risk and be able to act, Charles outlines a number of practical steps

1. **Engage your suppliers**. Asking vendors and other partners to report on their quantum preparedness provides you with valuable insights and highlights to your partner the importance of this issue, helping to spur future action.

2. **Audit your data**. Some of the data you encrypt today could be recoverable in the future. Audit what data is at risk of so-called store-and-decrypt attacks and ensure this data cannot be accessed in the first place. Alternatively, start deploying quantum-safe encryption alongside legacy algorithms.

3. **Review your digital signatures**. Do you rely on long-term public keys that cannot be upgraded? If so, your business will be at risk of signature forgery on the arrival of quantum computers. Now is the time to ensure all your keys can be upgraded in the future if required, or to put in place additional controls on digital signature usage.

Given the magnitude of this potential threat, HP advises IT leaders to demonstrate an abundance of caution. Charles concludes: "With regard to the quantum challenge, IT leaders should move forward cautiously and in a controlled manner from what we trust now to what we will trust in the future. Implement practical solutions while being aware of the usual vulnerabilities that can come with new systems."

2.World's First Room-Temperature Superconductor Synthesized, Could Impact Development of Quantum Computing and Qubits

https://quantumzeitgeist.com/worlds-first-room-temperature-superconductor-synthesized-could-impact-development-of-quantum-computing-and-qubits/

Scientists from South Korea have successfully synthesised a room-temperature superconductor, LK-99, that works at ambient pressure. This is a significant breakthrough, as previous room-temperature superconductors required extremely high pressure to function. The superconductivity of LK-99 is due to minute structural distortion caused by the substitution of Cu2+ ions in the insulating network of Pb(2)-phosphate, not by external factors such as temperature and pressure. This discovery could open up new possibilities for various applications such as magnets, motors, power cables, and of course, quantum computing.

The development will be of particular interest to those working on superconducting quantum devices where the qubits typically have to be cooled or refrigerated to a very low temperature. Devices such as those from IBM and Rigetti work using superconducting qubits. Whilst the news from the South Korean team still needs to be digested, the world's scientists are excited as the innovation could be transformative in so many fundamental areas. What is also apparent is that the materials used are not that exotic. Hence, if the results can be corroborated, then the materials could be widespread and embedded into many applications.

``For the first time in the world, we succeeded in synthesizing the room-temperature superconductor (Tc ≥ 400 K, 127^0C) working at ambient pressure with a modified lead-apatite (LK-99) structure."

Discovery of a Room-Temperature Superconductor

This superconductor, named LK-99, has a modified lead-apatite structure. The superconductivity of LK-99 is proven with the Critical temperature (Tc), Zero-resistivity, Critical current (Ic), Critical magnetic field (Hc), and the Meissner effect. The superconductivity of LK-99 originates from minute structural distortion by a slight volume shrinkage (0.48 %), not from external factors such as temperature and pressure.

Overcoming the High-Pressure Problem

The recent success of developing room-temperature superconductors with hydrogen sulfide and yttrium super-hydride has garnered worldwide attention. However, these superconductors are difficult to apply to actual application devices in daily life because of the tremendously high pressure required. To overcome this high-pressure problem, scientists have taken a chemical approach to synthesise a room-temperature and ambient-pressure superconductor, LK-99.

The Unique Structure of LK-99

The unique structure of LK-99 allows the minute distorted structure to be maintained in the interfaces. This is the most important factor that LK-99 maintains and exhibits superconductivity at room temperatures and ambient pressure. The shrinkage in LK-99 is caused by Cu2+ substitution of Pb2+(2) ions in the insulating network of Pb(2)-phosphate, and it generates stress. It concurrently transfers to Pb(1) of the cylindrical column resulting in distortion of the cylindrical column interface, which creates superconducting quantum wells (SQWs) in the interface.

The Role of Stress in Superconductivity

"For the first time in the world, we report the success in synthesizing a room-temperature and ambient-pressure superconductor with a chemical approach to solve the temperature and pressure problem."

The stress generated by the decrease in volume under low temperature or high pressure causes a minute strain or distortion. This structural change seems to bring about the superconductivity of it. The stress caused by temperature and pressure brings a minute structural distortion and strain, which cre-

ates an electronic state for superconductivity. In LK-99, the stress generated by the Cu2+ replacement of Pb(2)2+ ion was not relieved due to the structural uniqueness of LK-99 and at the same time was appropriately transferred to the interface of the cylindrical column.

Potential Applications of LK-99

LK-99 has many possibilities for applications such as magnets, motors, cables, levitation trains, power cables, qubits for a quantum computer, THz Antennas, etc. This new development is expected to be a significant historical event that opens a new era for humankind.

“All evidence and explanation lead that LK-99 is the first room-temperature and ambient-pressure superconductor. The LK-99 has many possibilities for various applications such as magnet, motor, cable, levitation train, power cable, qubit for a quantum computer, THz Antennas, etc. We believe that our new development will be a brand-new historical event that opens a new era for humankind.”

Quick Summary

Scientists have successfully synthesised a room-temperature superconductor, LK-99, that works at ambient pressure, a world-first achievement. The superconductivity of LK-99 is due to minute structural distortion caused by the substitution of copper ions, creating superconducting quantum wells and allowing it to maintain and exhibit superconductivity at room temperatures and ambient pressure.

- For the first time, a room-temperature superconductor (LK-99) has been successfully synthesised, working at ambient pressure.
- The superconductivity of LK-99 is proven with the Critical temperature (Tc), Zero-resistivity, Critical current (Ic), Critical magnetic field (Hc), and the Meissner effect.
- The superconductivity of LK-99 originates from minute structural distortion by a slight volume shrinkage (0.48 %), not by external factors such as temperature and pressure.
- The shrinkage is caused by Cu2+ substitution of Pb2+(2) ions in the insulating network of Pb(2)-phosphate, and it generates stress.
- The stress concurrently transfers to Pb(1) of the cylindrical column resulting in distortion of the cylindrical column interface, which creates superconducting quantum wells (SQWs) in the interface.
- The unique structure of LK-99 that allows the minute distorted structure to be maintained in the interfaces is the most important factor that LK-99 maintains and exhibits superconductivity at room temperatures and ambient pressure.
- The LK-99 has many possibilities for applications such as magnet, motor, cable, levitation train, power cable, qubits for a **quantum computer**, THz Antennas, etc.

3.U.S. Hunts Chinese Malware That Could Disrupt American Military Operations

by David E. Sanger and Julian E. Barnes
https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html

The Biden administration is hunting for malicious computer code it believes China has hidden deep inside the networks controlling power grids, communications systems and water supplies that feed military bases in the United States and around the world, according to American military, intelligence and national security officials.

The discovery of the malware has raised fears that Chinese hackers, probably working for the People's Liberation Army, have inserted code designed to disrupt U.S. military operations in the event of a conflict, including if Beijing moves against Taiwan in coming years.

The malware, one congressional official said, was essentially "a ticking time bomb" that could give China the power to interrupt or slow American military deployments or resupply operations by cutting off power, water and communications to U.S. military bases. But its impact could be far broader, because that same infrastructure often supplies the houses and businesses of ordinary Americans, according to U.S. officials.

The first public hints of the malware campaign began to emerge in late May, when Microsoft said it had detected mysterious computer code in telecommunications systems in Guam, the Pacific island with a vast American air base, and elsewhere in the United States. But that turned out to be only the narrow slice of the problem that Microsoft could see through its networks.

More than a dozen U.S. officials and industry experts said in interviews over the past two months that the Chinese effort goes far beyond telecommunications systems and predated the May report by at least a year. They said the U.S. government's effort to hunt down the code, and eradicate it, has been underway for some time. Most spoke on the condition of anonymity to discuss confidential and in some cases classified assessments.

They say the investigations so far show the Chinese effort appears more widespread — in the United States and at American facilities abroad — than they had initially realized. But officials acknowledge that they do not know the full extent of the code's presence in networks around the world, partly because it is so well hidden.

The discovery of the malware has touched off a series of Situation Room meetings in the White House in recent months, as senior officials from the National Security Council, the Pentagon, the Homeland Security Department and the nation's spy agencies attempt to understand the scope of the problem and plot a response.

Biden administration officials have begun to brief members of Congress, some state governors and utility companies about the findings, and confirmed some conclusions about the operation in interviews with The New York Times.

There is a debate inside the administration over whether the goal of the operation is primarily aimed at disrupting the military, or at civilian life more broadly in the event of a conflict. But officials say that the initial searches for the code have focused first on areas with a high concentration of American military bases.

In response to questions from The Times, the White House issued a statement Friday night that made no reference to China or the military bases.

"The Biden administration is working relentlessly to defend the United States from any disruptions to our critical infrastructure, including by coordinating interagency efforts to protect water systems, pipelines, rail and aviation systems, among others," said Adam R. Hodge, the acting spokesman for the National Security Council.

He added: "The president has also mandated rigorous cybersecurity practices for the first time." Mr. Hodge was referring to a series of executive orders, some motivated by concerns over SolarWinds, commercial software used widely by the U.S. government that was breached by a Russian surveillance operation, and the Colonial Pipeline ransomware attack by a Russian criminal group. That attack resulted in the temporary cutoff of half the gasoline, jet fuel and diesel supplies that

run up the East Coast.

The U.S. government and Microsoft have attributed the recent malware attack to Chinese state-sponsored actors, but the government has not disclosed why it reached that conclusion. There is debate among different arms of the U.S. government about the intent of the intrusions, but not about their source.

The public revelation of the malware operation comes at an especially fraught moment in relations between Washington and Beijing, with clashes that include Chinese threats against Taiwan and American efforts to ban the sale of highly sophisticated semiconductors to the Chinese government. Many of the tensions in the relationship have been driven not only by technological competition but by mutual accusations of malicious activity in cyberspace.

The United States has blamed China for a variety of major hacks against U.S. agencies and infrastructure, and accused the foreign power of spying from a bus-size balloon that traversed the United States in February, until it was shot down off South Carolina. For its part, China has accused the United States of hacking into Huawei, its telecommunications giant. Secret documents released a decade ago by Edward Snowden, a former National Security Agency contractor now in exile in Russia, confirmed that American intelligence agencies did just that.

But almost all of those cases involved intelligence gathering. The discovery of the malicious code in American infrastructure, one of Mr. Biden's most senior advisers said, "raises the question of what, exactly, they are preparing for."

If gaining advantage in a Taiwan confrontation is at the heart of China's intent, slowing down American military deployments by a few days or weeks might give China a window in which it would have an easier time taking control of the island by force.

Chinese concern about American intervention was most likely fueled by President Biden's several statements over the past 18 months that he would defend Taiwan with American troops if necessary.

Another theory is that the code is intended to distract. Chinese officials, U.S. intelligence agencies have assessed, may believe that during an attack on Taiwan or other Chinese action, any interruptions in U.S. infrastructure could so fixate the attention of American citizens that they would think little about an overseas conflict.

The Chinese embassy in Washington issued a statement on Saturday after publication of this article, denying that it engages in hacking and accusing the United States of being a far larger offender. "We have always firmly opposed and cracked down on all forms of cyberattacking in accordance with the law," said Haoming Ouyang, an embassy spokesman.

"The Chinese government agencies face numerous cyberattacks every day, most of which come from sources in the U.S.," he wrote, adding: "We hope relevant parties will stop smearing China with groundless accusations."

Chinese officials have never conceded that China was behind the theft of security clearance files of roughly 22 million Americans — including six million sets of fingerprints — from the Office of Personnel Management during the Obama administration. That exfiltration resulted in an agreement between President Obama and President Xi Jinping that resulted in a brief decline in malicious Chinese cyberactivity. The agreement has since collapsed.

Now, Chinese cyberoperations seem to have taken a turn. The latest intrusions are different from those in the past because disruption, not surveillance, appears to be the objective, U.S. officials say.

At the Aspen Security Forum earlier this month, Rob Joyce, the director of cybersecurity at the National Security Agency, said China's recent hack targeting the American ambassador to Beijing, Nicholas Burns, and the commerce secretary, Gina Raimondo, was traditional espionage. The spy balloon shot down earlier this year also captured public attention, but generated less concern inside the intelligence community. Intelligence officials and others in the Biden administration viewed those operations as the kind of spy-versus-spy games that Washington and Beijing have run against each other for decades.

In contrast, Mr. Joyce said the intrusions in Guam were "really disturbing" because of their disruptive potential.

The Chinese code, the officials say, appears directed at ordinary utilities that serve both civilian populations and nearby military bases. Only America's nuclear sites have self-contained communication systems, electricity and water pipelines. (The code has not been found in classified systems. Officials declined to describe the unclassified military networks in which the code has been found.)

While the most sensitive planning is carried out on classified networks, the military routinely uses unclassified, but secure, networks for basic communications, personnel matters, logistics and supply issues.

Officials say that if the malware is activated, it is not clear how effective it would be at slowing an American response — and that the Chinese government may not know, either. In interviews, officials said they believe that in many cases the communications, computer networks and power grids could be quickly restored in a matter of days.

But intelligence analysts have concluded that China may believe there is utility in any disruptive attack that could slow down the U.S. response.

The initial Microsoft discovery in Guam — home to major U.S. Air Force and Marine bases — was attributed by the company to a Chinese state-sponsored hacking group that the company named Volt Typhoon.

A warning from the Homeland Security Department's Cybersecurity and Infrastructure Security Agency, the National Security Agency and others issued the same day also said the malware was from the state-sponsored Chinese hacking group and was "living off the land." The phrase means that it was avoiding detection by blending in with normal computer activity, conducted by authorized users. But the warning did not outline other details of the threat.

Some officials briefly considered whether to leave the malware in place, quietly monitor the code they had found and prepare plans to try to neutralize it if it was even activated. Monitoring the intrusions would allow them to learn more about it, and possibly lull the Chinese hackers into a false sense that their penetration had not been exposed.

But senior White House officials quickly rejected that option and said that given the potential threat, the prudent path was to excise the offending malware as quickly as it could be found.

Still, there are risks.

American cybersecurity experts are able to remove some of the malware, but some officials said there are concerns that the Chinese could use similar techniques to quickly regain access.

Removing the Volt Typhoon malware also runs the risk of tipping off China's increasingly talented hacking forces about what intrusions the United States is able to find, and what it is missing. If that happens, China could improve its techniques and be able to reinfect military systems with even harder-to-find software.

The recent Chinese penetrations have been enormously difficult to detect. The sophistication of the attacks limits how much the implanted software is communicating with Beijing, making it difficult to discover. Many hacks are discovered when experts track information being extracted out of a network, or unauthorized accesses are made. But this malware can lay dormant for long periods of time.

Speaking earlier this month at an intelligence summit, George Barnes, the deputy director of the National Security Agency, said the Volt Typhoon attacks demonstrated how much more sophisticated China had become at penetrating government and private sector networks.

Mr. Barnes said that rather than exploit flaws in software to gain access, China had found ways to steal or mimic the credentials of system administrators, the people who run computer networks. Once those are in hand, the Chinese hackers essentially have the freedom to go anywhere in a network and implant their own code.

“China is steadfast and determined to penetrate our governments, our companies, our critical infrastructure,” Mr. Barnes said.

“In the earlier days, China’s cyberoperations activities were very noisy and very rudimentary,” he continued. “They have continued to bring resources, sophistication and mass to their game. So the sophistication continues to increase.”

4.Cryptography may offer a solution to the massive AI-labeling problem

by Tate Ryan-Mosley
https://www.technologyreview.com/2023/07/28/1076843/cryptography-ai-labeling-problem-c2pa-provenance/

The White House wants big AI companies to disclose when content has been created using artificial intelligence, and very soon the EU will require some tech platforms to label their AI-generated images, audio, and video with “prominent markings” disclosing their synthetic origins.

There’s a big problem, though: identifying material that was created by artificial intelligence is a massive technical challenge. The best options currently available—detection tools powered by AI, and watermarking—are inconsistent, impermanent, and sometimes inaccurate. (In fact, just this week OpenAI shuttered its own AI-detecting tool because of high error rates.)

But another approach has been attracting attention lately: C2PA. Launched two years ago, it’s an open-source internet protocol that relies on cryptography to encode details about the origins of a piece of content, or what technologists refer to as “provenance” information.

The developers of C2PA often compare the protocol to a nutrition label, but one that says where content came from and who—or what—created it.

The project, part of the nonprofit Joint Development Foundation, was started by Adobe, Arm, Intel, Microsoft, and Truepic, which formed the Coalition for Content Provenance and Authenticity (from which C2PA gets its name). Over 1,500 companies are now involved in the project through the closely affiliated open-source community, Content Authenticity Initiative (CAI), including ones as varied and prominent as

Nikon, the BBC, and Sony.

Recently, as interest in AI detection and regulation has intensified, the project has been gaining steam; Andrew Jenks, the chair of C2PA, says that membership has increased 56% in the past six months. The major media platform Shutterstock has joined as a member and announced its intention to use the protocol to label all its AI-generated content, including its DALL-E-powered AI image generator.

Sejal Amin, chief technology officer at Shutterstock, told MIT Technology Review in an email that the company is protecting artists and users by "supporting the development of systems and infrastructure that create greater transparency to easily identify what is an artist's creation versus AI-generated or modified art."

What is C2PA and how is it being used?

Microsoft, Intel, Adobe, and other major tech companies started working on C2PA in February 2021, hoping to create a universal internet protocol that would allow content creators to opt in to labeling their visual and audio content with information about where it came from. (At least for the moment, this does not apply to text-based posts.)

Crucially, the project is designed to be adaptable and functional across the internet, and the base computer code is accessible and free to anyone.

Truepic, which sells content verification products, has demonstrated how the protocol works with a deepfake video with Revel.ai. When a viewer hovers over a little icon at the top right corner of the screen, a box of information about the video appears that includes the disclosure that it "contains AI-generated content."

Adobe has also already integrated C2PA, which it calls content credentials, into several of its products, including Photoshop and Adobe Firefly. "We think it's a value-add that may attract more customers to Adobe tools," Andy Parsons, senior director of the Content Authenticity Initiative at Adobe and a leader of the C2PA project, says.

C2PA is secured through cryptography, which relies on a series of codes and keys to protect information from being tampered with and to record where information came from. More specifically, it works by encoding provenance information through a set of hashes that cryptographically bind to each pixel, says Jenks, who also leads Microsoft's work on C2PA.

C2PA offers some critical benefits over AI detection systems, which use AI to spot AI-generated content and can in turn learn to get better at evading detection. It's also a more standardized and, in some instances, more easily viewable system than watermarking, the other prominent technique used to identify AI-generated content. The protocol can work alongside watermarking and AI detection tools as well, says Jenks.

The value of provenance information

Adding provenance information to media to combat misinformation is not a new idea, and early research seems to show that it could be promising: one project from a master's student at the University of Oxford, for example, found evidence that users were less susceptible to misinformation when they had access to provenance information about content. Indeed, in OpenAI's update about its AI detection tool, the company said it was focusing on other "provenance techniques" to meet disclosure requirements.

That said, provenance information is far from a fix-all solution. C2PA is not legally binding, and without required internet-wide adoption of the standard, unlabeled AI-generated content will exist, says Siwei Lyu, a director of the Center for Information Integrity and professor at the University at Buffalo in New

York. “The lack of over-board binding power makes intrinsic loopholes in this effort,” he says, though he emphasizes that the project is nevertheless important.

What’s more, since C2PA relies on creators to opt in, the protocol doesn’t really address the problem of bad actors using AI-generated content. And it’s not yet clear just how helpful the provision of metadata will be when it comes to media fluency of the public. Provenance labels do not necessarily mention whether the content is true or accurate.

Ultimately, the coalition’s most significant challenge may be encouraging widespread adoption across the internet ecosystem, especially by social media platforms. The protocol is designed so that a photo, for example, would have provenance information encoded from the time a camera captured it to when it found its way onto social media. But if the social media platform doesn’t use the protocol, it won’t display the photo’s provenance data.

The major social media platforms have not yet adopted C2PA. Twitter had signed on to the project but dropped out after Elon Musk took over. (Twitter also stopped participating in other volunteer-based projects focused on curbing misinformation.)

C2PA “[is] not a panacea, it doesn’t solve all of our misinformation problems, but it does put a foundation in place for a shared objective reality,” says Parsons. “Just like the nutrition label metaphor, you don’t have to look at the nutrition label before you buy the sugary cereal.

“And you don’t have to know where something came from before you share it on Meta, but you can. We think the ability to do that is critical given the astonishing abilities of generative media.”

5.BTQ Technologies Corp.’s Post-Quantum Cryptography Scheme Preon Selected by NIST

by Donovan Johnson
https://fagenwasanni.com/news/btq-technologies-corp-s-post-quantum-cryptography-scheme-preon-selected-by-nist/87740/

BTQ Technologies Corp.’s post-quantum cryptography scheme, **Preon**, has been selected by the National Institute of Standards and Technology (NIST) in the first round for consideration in their Post-Quantum Cryptography (PQC) standardization process. Preon is a robust and efficient post-quantum signature scheme that offers small key size, rapid key generation, minimal assumptions, and flexible functionality. These features make it resistant to potential threats from both classical and quantum computers.

The selection of Preon highlights the innovative work of BTQ Technologies Corp. in developing highly secure cryptographic schemes. It reinforces the company’s commitment to protecting digital infrastructures against potential quantum threats.

Preon, co-authored by Hon Hai Research Institute, the research arm of Hon Hai Precision Industry Co., Ltd. (Foxconn), is a post-quantum signature scheme that is resilient against classical and quantum attacks. It operates based on a general proving system that requires minimal assumptions. The scheme

has a small key size, quick key generation process, and flexible functionality. It supports features like selective-reveal or threshold signature due to its construction based on a zero-knowledge proof.

The National Institute of Standards and Technology (NIST) has been engaged in a public process since December 2016 to select quantum-resistant public-key cryptographic algorithms for standardization. This process aims to combat the threats posed by the rapid advancement of quantum computing. Several algorithms have already been standardized, and Preon's selection in the PQC standardization process further contributes to the development of secure cryptographic solutions.

BTQ Technologies Corp. is a global quantum technology company that focuses on securing mission-critical networks. The company combines software and hardware to provide unique post-quantum services and solutions. It collaborates with leading research institutes and universities to create innovative approaches to address the security challenges posed by large-scale universal quantum computers.

Overall, the selection of Preon by NIST for consideration in their PQC standardization process demonstrates the industry's commitment to developing advanced cryptographic schemes capable of withstanding potential threats from quantum computers.

6.A Brief Overview of Quantum Computing in South Korea in 2023

by James Dargan
https://thequantuminsider.com/2023/07/28/a-brief-overview-of-quantum-computing-in-south-korea-in-2023/

The announcement earlier this year that South Korea plans to invest over 3 trillion won ($2.33 billion) in quantum science and technology by 2035 is a sure sign the country intends to become a global leader in the field. It will do this by increasing the number of quantum researchers seven-fold to 2,500 and developing its own quantum computer and advanced quantum sensors, as well as securing ten percent of the global market share in quantum technology by 2035, signing partnerships with IBM and IonQ in the process to train local experts in the technology.

South Korea, just like other countries in the region, has been actively involved in quantum technology research and development for decades now and can boast a healthy ecosystem—not only at the national level with several initiatives and institutions in the country dedicated to advancing this field—but with private companies, too.

We will now take a brief look at what is going on in the country as of mid-2023.

Government Position

The Korea Institute of Science and Technology (KIST) is one of the major players in quantum computing in South Korea. Over the last several years, KIST has been conducting research in quantum information processing and quantum computing. In addition to developing quantum algorithms, hardware and software, they explore potential applications of quantum computing.

Furthermore, universities, industries and government agencies are collaborating to promote quantum computing in South Korea. To support quantum technologies research, development, and commercialization, the South Korean government launched the Quantum Computing Development Strategy. Re-

searchers are funded to conduct research, testbeds are created and industry and academia collaborate on research.

Another interesting point to mention is the fact that IonQ has signed an agreement with South Korea's Ministry of Science and ICT to cultivate the regional quantum computing ecosystem.

Research

South Korea has been increasing its focus on quantum technology and has been supportive by providing funding and incentives to those involved in this field. There are several universities in South Korea that have established quantum computing research centres or laboratories in addition to KIST. The following are some of the most important players in the Korean quantum technology ecosystem:

Seoul National University, for example, conducts research on quantum algorithms, error correction, and quantum simulation. Research on quantum computing and related areas is also carried out at the Quantum Information and Computation Laboratory at KAIST (Korea Advanced Institute of Science and Technology). Students interested in quantum computing can participate in KAIST's research and education programs. Through the IBM Quantum Network, KAIST will enhance Korean technology's global position in quantum computing by exchanging information with other organizations and corporations

Another worth mentioning is the Sungkyunkwan University (SKKU) — Quantum Information Research Support Center (Q-Center), which was established by the Ministry of Science and ICT's project to create a quantum information ecosystem.

Yonsei University's Institute for Quantum Information Technology (IQIT) aims to enrich human life through quantum information research, as well as prepare for the future information society by developing quantum ecosystems and teaching quantum information technology. Researchers at Yonsei University are advancing the frontiers of quantum computing by conducting cutting-edge research in the areas of software development, algorithm development, and quantum ecosystem development.

Private Sector

There are also several South Korean companies that are actively involved in quantum computing. Quantum computing has sparked interest among global corporations with companies such as Samsung, SK Telecom and LG Electronics interested in the technology. Their R&D efforts are focused on the development of quantum computers, quantum algorithms and quantum communication systems.

Smaller startup companies are in on the act, too.

Based in Seoul, South Korea, with additional offices in Arlington, Virginia, EYL was founded in 2015 and provides a tiny quantum random number generator chip that measures 5 millimetres. Besides developing an ultralight chip encryptor for all IoT devices, EYL is also developing a thin film-type quantum random generator for identification cards and credit cards.

Using their proprietary quantum Karnaugh map-based optimization protocol and intellectual properties, First Quantum offers solutions for core quantum computing applications. Located in Seoul, First Quantum was founded in 2022. In particular, the company is interested in the computational fluid dynamics governed by the Navier-Stokes nonlinear partial differential equations whose solution is fundamental to the aerospace industry, astrophysics and numerical weather and climate prediction. The company is conducting further research on quantum algorithms for financial engineering problems such as portfolio optimization and derivative pricing.

QSIMPLUS offers a product called QSIMpro, a software simulator for cryptographic communication. By eliminating the need for typically necessary hardware, this product reduces time and costs. Non-experts

in quantum communication can implement and verify various QC systems by dragging and dropping blocks that behave similarly to hardware components. The company was founded in 2021 and is based in Seoul.

Another important company in the country is Qunova Computing, which provides software services to clients in the pharmaceutical discovery and materials industries. Founded in Daejeon in 2021, Qunova's quantum software solutions allow clients to save significant amounts of time in their research and development processes, identifying candidate materials and drugs with the desired properties much faster, thereby reducing costs and maximizing resources.

Though not a private company, SK Telecom has been investing in quantum computing and has established the Spin Quantum Computing Center with Korea University and the California Institute of Technology.

Another public company in the picture is Samsung, which has been investing in quantum computing and working on developing its own quantum computer.

Key People

Picking the most important people in any industry is a difficult thing to do, but we managed to choose two individuals whose contribution is driving the country forward in quantum technology.

Hyunseok Jeong is a professor at the Department of Physics and Astronomy at Seoul National University and leads the Quantum Information Science Group in the Department of Physics and Astronomy at the university. He has contributed significantly to the field of quantum optics and quantum information, particularly in quantum teleportation and quantum repeaters.

A professor at the School of Electrical Engineering, KAIST (Korea Advanced Institute of Science and Technology), Jaewan Kim has made notable contributions to the development of quantum communication technologies, including quantum key distribution (QKD) and quantum hacking detection.

Conclusion

The unveiling by the South Korean Ministry of Science and ICT (MSIT) of its comprehensive "Quantum Science and Technology Strategy" signifies a significant milestone for the country. This ambitious plan, aimed at propelling South Korea as a global hub for the quantum economy by 2035, underscores the country's commitment to making up for its relatively late entry into the quantum field. The strategy covers an expansive range of applications from quantum computing and quantum internet to quantum sensors.

Importantly, this initiative, one of the top five publicly disclosed quantum commitments globally, acknowledges South Korea's current technological deficit and outlines a robust plan to achieve quantum parity with leading countries by 2035. South Korea's objective to train up to 2,500 quantum professionals, foster global quantum market signals the nation's deep commitment to this emerging sector.

Also noteworthy are the strategic partnerships that the ministry plans to build with quantum tech companies including IBM and IonQ. These collaborations with industry leaders can be instrumental in accelerating South Korea's quantum advancement. The country is also expanding its international cooperation investment to KRW 210 billion for 2023–2025, marking a substantial increase from the KRW 13 billion allocated for 2019–2022.

However, not everything is on a positive note, as an article last year published in *The Korea Economic Daily* criticized Seoul's quantum computer development efforts, stating that the country lacks an industrial ecosystem in the quantum computing field.

In summary, while South Korea acknowledges it is playing catch-up in quantum technology relative to other countries, its ambitious and comprehensive strategy, significant financial commitment, and strategic partnerships could help it close the gap and potentially emerge as a significant player in the global quantum economy.

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

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

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

7.Russian Scientists Present 16-Qubit Quantum Computer

by Matt Swayne
https://thequantuminsider.com/2023/07/25/russian-company-presents-16-qubit-quantum-computer/

A team of Russian physicists presented a 16-qubit quantum computer at the Forum for Future Technologies in Russia that appears to combine trapped ion and photonics approaches, according to a post from Rosatom, the Russian State Nuclear Energy Corporation .

The computer is the first quantum computer developed in Russia, according to the post, which was translated into English by a computer.

The device is still in the early stages of development and is small by standards already achieved by global quantum leaders. However, it has the potential to be a powerful tool for research and development, the scientist said. The team added that they have already used the device for simulating simple molecules.

The development of quantum computers is a major technological advance, and it is likely to have a significant impact on a wide range of industries. Russia's investment in quantum computing is a sign of the country's commitment to this emerging technology.

The program officially began in 2019, according to the article. However, Ilya Semerikov, a researcher at the LPI Laboratory of Optics of Complex Quantum Systems, said that work on the trapped ion device started as early as 2015. The team first built a quantum clock for GLONASS, a Russian global positioning system.

"There was a big discussion about whether to include our ion platform in it. And I am grateful to

Rosatom, who believed in us then," Semerikov said in the post. "Our quantum computer, which is important, is already doing useful things – modeling molecules, and is not engaged in scientific abstraction."

At the demonstration, Russian President Vladimir Putin — maybe joking, maybe not — said that the important thing now was for the researchers to not retire.

In addition to this device, Russia is also developing other quantum computers. Among other programs, the Russian government announced in 2021 that it would invest $790 million in quantum computing research over the next five years. This investment is part of a larger effort by Russia to develop its technological capabilities and become a leader in the global economy.

The development of quantum computers is a race between different countries, and Russia is not the only one that is investing heavily in this technology. The United States, China and the European Union are also investing billions of dollars in quantum computing research.

The winner of the quantum computing race will have a significant advantage in a number of industries, including cryptography, materials science and drug discovery.

8.Chinese Scientists Say Metropolitan Quantum Teleportation Reaches Hertz Rate

by Matt Swayne
https://thequantuminsider.com/2023/07/25/chinese-scientists-say-metropolitan-quantum-teleportation-reaches-hertz-rate/

Quantum teleportation allows quantum information to be transferred to a remote location by using quantum entanglement and classical communication. It has been achieved with different degrees of freedom of quantum light from table-top experiments to real-world demonstrations. Especially, using a low-Earth orbit Micius satellite, researchers have achieved quantum teleportation over 1200 km. While, to date, there is no quantum teleportation system, whose rate can reach the order of Hertz. This hinders future applications of quantum internet.

In a paper published in Light Science & Application, a team of scientists, led by Prof. Guangcan Guo and Prof. Qiang Zhou from the University of Electronic Science and Technology of China (UESTC) cooperating with Prof. Lixing You from the Shanghai Institute of Microsystem and Information Technology of the Chinese Academy of Sciences, have improved the teleportation rate to 7.1 qubits per second for the first time based on the "No. 1 Metropolitan Quantum Internet of UESTC". This presents a new record for the quantum teleportation system over metropolitan range.

"Demonstrating high-speed quantum teleportation outside of a laboratory involves a whole set of challenges. This experiment shows how these challenges can be overcome and hence it establishes an important milestone towards the future quantum internet." said Prof. Qiang Zhou, who is the corresponding author of this work. The main experimental challenge in a real-world quantum teleportation system is performing the Bell state measurement (BSM). In order to ensure the successful quantum teleportation and improve the efficiency of BSM, Alice's and Bob's photons need to be indistinguishable at Charlie after long-distance transmission in fiber. The team developed a fully running feedback system, which

realized the fast stabilization of the path length difference and polarization of the photons.

On the other hand, the team used a single piece of fiber-pigtailed periodically poled lithium niobate waveguide to generate the entangled photon pairs. Based on this, a high-quality quantum entangled light source with 500 MHz repetition rate was developed for the teleportation system.

Such a high-speed quantum teleportation based on quantum optics requires the most sensitive photon sensors in order to collect as many events as possible. The team led by Prof. Lixing You, along with colleagues of Photon Technology Co., LTD, provided high performance superconducting nanowire single-photon detectors for the experiment. Benefiting from the detectors with excellent efficiency and almost no noise, high-efficiency BSM and quantum state analysis were achieved.

The team employed both quantum state tomography and decoy state method to calculate the teleportation fidelities, which were well above the classical limit (66.7%), confirming that high-speed metropolitan quantum teleportation has been achieved.

The “No. 1 Metropolitan Quantum Internet of UESTC” is expected to develop a “high speed, high fidelity, multi users, long distance” quantum internet infrastructure in the future by combining integrated quantum light sources, quantum repeaters, and quantum information nodes. The team also forecasts that this infrastructure will further promote the practical application of quantum internet.

9.Researchers Find ‘Backdoor’ in Encrypted Police and Military Radios

by Joseph Cox
https://www.vice.com/en/article/4a3n3j/backdoor-in-police-radios-tetra-burst

A group of cybersecurity researchers has uncovered what they believe is an intentional backdoor in encrypted radios used by police, military, and critical infrastructure entities around the world. The backdoor may have existed for decades, potentially exposing a wealth of sensitive information transmitted across them, according to the researchers.

While the researchers frame their discovery as a backdoor, the organization responsible for maintaining the standard pushes back against that specific term, and says the standard was designed for export controls which determine the strength of encryption. The end result, however, are radios with traffic that can be decrypted using consumer hardware like an ordinary laptop in under a minute.

“There's no other way in which this can function than that this is an intentional backdoor,” Jos Wetzels, one of the researchers from cybersecurity firm Midnight Blue, told Motherboard in a phone call.

The research is the first public and in-depth analysis of the TErrestrial Trunked RAdio (TETRA) standard in the more than 20 years the standard has existed. Not all users of TETRA-powered radios use the specific encryption algorithim called TEA1 which is impacted by the backdoor. TEA1 is part of the TETRA standard approved for export to other countries. But the researchers also found other, multiple vulnerabilities across TETRA that could allow historical decryption of communications and deanonymization. TETRA-radio users in general include national police forces and emergency services in Europe; military organizations in Africa; and train operators in North America and critical infrastructure providers elsewhere.

Midnight Blue will be presenting their findings at the upcoming Black Hat cybersecurity conference in August. The details of the talk have been closely under wraps, with the Black Hat website simply describing the briefing as a "Redacted Telecom Talk." That reason for secrecy was in large part due to the unusually long disclosure process. Wetzels told Motherboard the team has been disclosing these vulnerabilities to impacted parties so they can be fixed for more than a year and a half. That included an initial meeting with Dutch police in January 2022, a meeting with the intelligence community later that month, and then the main bulk of providing information and mitigations being distributed to stakeholders. NLnet Foundation, an organization which funds "those with ideas to fix the internet," financed the research.

The European Telecommunications Standards Institute (ETSI), an organization that standardizes technologies across the industry, first created TETRA in 1995. Since then, TETRA has been used in products, including radios, sold by Motorola, Airbus, and more. Crucially, TETRA is not open-source. Instead, it relies on what the researchers describe in their presentation slides as "**secret, proprietary cryptography**," meaning it is typically difficult for outside experts to verify how secure the standard really is.

The researchers said they worked around this limitation by purchasing a TETRA-powered radio from eBay. In order to then access the cryptographic component of the radio itself, Wetzels said the team found a vulnerability in an interface of the radio. From there, they achieved code execution on the main application processor; they then jumped to the signals processor, which Wetzels described as something equivalent to a wifi or 3G chip, which handles the radio's signals. On that chip, a secure enclave held the cryptographic ciphers themselves. The team finally found vulnerabilities in that which allowed them to extract the cryptography and perform their analysis. The team then reverse-engineered how TETRA implemented its cryptography, which led to the series of vulnerabilities that they have called TETRA:BURST. "It took less time than we initially expected," Wetzels said.

Most interestingly is the researchers' findings of what they describe as the backdoor in TEA1. Ordinarily, radios using TEA1 used a key of 80-bits. But Wetzels said the team found a "secret reduction step" which dramatically lowers the amount of entropy the initial key offered. An attacker who followed this step would then be able to decrypt intercepted traffic with consumer-level hardware and a cheap software defined radio dongle.

"This is a trivial type of attack that fully breaks the algorithm. That means an attacker can passively decrypt everything in almost real time. And it's undetectable, if you do it passively, because you don't need to do any weird interference stuff," Wetzels said.

Not all current TETRA-radio customers will use TEA1, and some may have since moved onto TETRA's other encryption algorithms. But given TETRA's long life span, its existence still means there may have been room for exploitation if another party was aware of this issue.

"There's bigger fish who likely found this much earlier," Wetzels said, referring to other third parties who may have discovered the issue.

The researchers say they identified multiple entities that they believe may have used TEA1 products at some point. They include U.S. Africom, a part of the U.S. military which focuses on the continent. Multiple military agencies did not respond to Motherboard's request for comment.

"In the interest of public safety, we do not share detailed information on our cybersecurity infrastructure," Lenis Valens, a spokesperson for PANYNJ which manages JFK airport, said in a statement when asked if the organization used TETRA radios when contacted by Motherboard. "The agency has robust protocols in place and employs the latest technologies and best practices. Safety for our passengers and customers always comes first," the statement said.

Most law enforcement agencies contacted by Motherboard did not respond to a request for comment. Swedish authorities declined to comment.

Several radio manufacturers directed Motherboard to ETSI for comment. Claire Boyer, press and media officer for ETSI, told Motherboard in an email that “As the authority on the ETSI TETRA technology standard, we welcome research efforts that help us further develop and strengthen the security of the standard so that it remains safe and resilient for decades to come. We will respond to the report when it has been published.”

Specifically on the researchers’ claims of a backdoor in TEA1, Boyer added “At this time, we would like to point out that the research findings do not relate to any backdoors. The TETRA security standards have been specified together with national security agencies and are designed for and subject to export control regulations which determine the strength of the encryption.”

The researchers stressed that the key reduction step they discovered is not advertised publicly.

“‘Intentional weakening’ without informing the public seems like the definition of a backdoor,” Wouter Bokslag from Midnight Blue told Motherboard in an email.

In ETSI’s statement to Motherboard, Boyer said “there have not been any known exploitations on operational networks” of the vulnerabilities the researchers disclosed.

Bokslag from Midnight Blue said in response that “There is no reason ETSI would be aware of exploitations in the wild, unless customers reach out to ETSI after detecting anomalies in their network traffic.” Then with the TEA1 issues specifically, “since it can be passively intercepted and decrypted, there is no detectable interference, and ETSI not knowing any concrete cases seems like a bit of a meaningless statement with this regard.”

In response to some of the researchers’ findings, radio manufacturers have developed firmware updates for their products. For TEA1, however, the researchers recommend users migrate to another TEA cipher or apply additional end-to-end encryption to their communications. Wetzels said that such an add-on does exist, but that hasn’t been vetted by outside experts at this time.

Bart Jacobs, a professor of security, privacy and identity, who did not work on the research itself but says he was briefed on it, said he hopes “this really is the end of closed, proprietary crypto, not based on open, publicly scrutinised standards.”

10.Post-Quantum Cryptography: A Decade of Revolutionizing Internet Security

https://fagenwasanni.com/news/post-quantum-cryptography-a-decade-of-revolutionizing-internet-security/54458/

Over the past decade, the field of internet security has undergone a significant transformation, largely due to the advent of post-quantum cryptography. This revolutionary technology has redefined the way we protect our digital assets, offering a robust shield against the ever-evolving threats of the cyber world.

Post-quantum cryptography, also known as quantum-resistant cryptography, is a type of encryption that is designed to secure data against both classical and quantum computers. Traditional cryptographic systems, such as RSA and ECC, are vulnerable to quantum attacks. Quantum computers, with their su-

perior computational power, can easily crack these systems, posing a serious threat to internet security. However, post-quantum cryptography, with its quantum-resistant algorithms, promises to counter this threat effectively.

The impact of post-quantum cryptography on internet security over the past decade has been profound. It has not only enhanced the security of digital communications but also bolstered the confidence of businesses and individuals in the digital space. With the rise of e-commerce, online banking, and digital currencies, the need for robust internet security has never been greater. Post-quantum cryptography has stepped up to meet this demand, providing a secure foundation for digital transactions.

Moreover, post-quantum cryptography has also played a pivotal role in safeguarding national security. Governments around the world have recognized the potential of quantum computers to compromise national security by breaking traditional encryption systems. In response, they have started investing heavily in post-quantum cryptography. For instance, the National Institute of Standards and Technology (NIST) in the United States has been actively promoting research and development in this field.

However, the journey of post-quantum cryptography over the past decade has not been without challenges. The development and implementation of quantum-resistant algorithms is a complex process that requires significant computational resources. Additionally, these algorithms need to be thoroughly tested and validated to ensure their security against quantum attacks. Despite these challenges, the progress made in this field has been remarkable.

The future of post-quantum cryptography looks promising. As quantum computers become more powerful and accessible, the need for quantum-resistant encryption will only increase. Researchers are already working on developing more efficient and secure post-quantum algorithms. Furthermore, standardization efforts are underway to establish universal standards for post-quantum cryptography. These efforts will not only enhance the security of digital communications but also facilitate the adoption of this technology across various sectors.

In conclusion, the past decade has witnessed a revolution in internet security, driven by the advent of post-quantum cryptography. This technology has provided a robust defense against the threats posed by quantum computers, thereby enhancing the security of digital communications. Despite the challenges, the progress made in this field has been significant, and the future looks promising. As we move forward, post-quantum cryptography will continue to play a crucial role in safeguarding our digital world.

11.Emerging synergies: Leveraging AI to bolster post-quantum cryptographic security

by Joseph Pirone
https://federalnewsnetwork.com/commentary/2023/07/emerging-synergies-leveraging-ai-to-bolster-post-quantum-cryptographic-security/

In the world of quantum computers, the need for an advanced approach to cybersecurity is more necessary than ever. As a result, thought leaders in the post-quantum cryptography (PQC) space are looking for ways to utilize artificial intelligence to enhance and harden their cryptographic systems. Together, PQC and AI have the potential to increase the security of our digital systems in numerous ways. More

specifically, these two fields combined can augment threat detection, strengthen anomaly detection, provide dynamic algorithm changing, and optimize cryptographic key rotation algorithms.

First, it is critical to understand the quantum threat. It refers to the potential risk posed by quantum computers, which could compromise the security of the world's encrypted information by breaking the cryptographic algorithms currently used to protect it. Quantum computers are computing machines that leverage the principles of quantum mechanics to perform specific computational tasks exponentially faster than classical computers. Importantly, using Shor's algorithm, quantum computers can efficiently factor integers and solve the discrete logarithmic problem, which is assumed to be computationally infeasible today and therefore is the foundation of many cryptographic algorithms. In academia, it is believed that there is a high possibility a quantum computer will be able to break classic encryption within 10 years or less. When fully developed, it would allow for an adversary to have complete access to sensitive information such as bank account details, medical records and classified government data.

As the capabilities of quantum computers are ramping up, the world must act now. It is well known that adversaries and governments are currently storing data with the intention of using a quantum computer to decrypt and potentially exploit it. In the cryptography field, this is called Store Now, Decrypt Later (SNDL) and is a primary motivator as to why we need large-scale adoption of post-quantum cryptography now. The companies and governments who wait to implement PQC run the risk of adversaries obtaining even more sensitive data than they already have. It is not a matter of "if" our data will be decrypted, it's a matter of "when" and "how much."

As stated above, quantum computers threaten the security of many industries such as financial, medical and other areas where sensitive data must remain private. The quantum age is inevitable and coming fast. At the lowest level, the difference between an encryption algorithm for classical computing and a post-quantum algorithm is that a post-quantum algorithm is just a more complex math problem. However, at the highest level we have the potential to make fundamental alterations to the standard of our encryption solutions. As the world transitions, we have an opportunity to adopt a more modern cryptographic solution that utilizes a subset of artificial intelligence-machine learning to be anticipatory and adaptive to different threats based on different models of risk scores and policy evaluations.

Threat detection is one of the key ways we can enhance the security of a cyber system with ML. Threat detection refers to the ability to identify and respond to cybersecurity threats in real-time. Just as ML can expand the capabilities of PQC solutions, AI when coupled with quantum computers has the potential to create new complex and modern cybersecurity threats. Therefore, threat detection has become an essential component of any cybersecurity strategy. ML can assist in threat detection by analyzing large volumes of data from various internal sources in real-time. By leveraging machine learning algorithms, a model can identify patterns in the network traffic or data that may indicate a potential threat.

Similar to threat detection, cyber anomaly detection refers to the ability to identify unusual or unexpected events that may indicate a potential threat. Traditional cybersecurity systems rely on predefined rules to detect anomalies, but these rules may not be effective against the new and emerging cybersecurity risks that quantum computers are bringing to the cyber field. It is imperative for cybersecurity systems to become faster and smarter as the threats are getting faster and smarter. Both anomaly and threat detection are imperative for a healthy cryptographic system as they will be the first line of defense against the unprecedented threats posed by quantum computing.

Furthermore, ML can play a significant role in enhancing post-quantum cryptography solutions by enabling cryptographic algorithm swapping. Post-quantum cryptography is designed to be resistant to quantum attacks, using mathematical problems that are believed to be quantum resilient. There are currently multiple different algorithms going through the National Institute of Standards and Technology's screening process, including KYBER, Falcon and BIKE. However, with the advancement of technology, it is possible that these algorithms will also become vulnerable to quantum attacks in the future. This points to the critical importance of having a cryptographic system that is agnostic to which algorithm it

uses. ML can help identify the best algorithm to use for a given situation, optimize it for efficiency and security, and automatically swap the key algorithm. By integrating ML into PQC solutions, we can enhance the security of our data and ensure that our systems are resilient to the ever-evolving threat landscape.

Additionally, cryptographic key rotation is a technique used to secure data by replacing the original key with a new one. However, choosing the appropriate key and determining when to swap it on the fly can be a complex task. This is where an ML model comes in. By analyzing network traffic, ML algorithms can identify anomalous behavior and recommend the appropriate cryptographic key to use. For example, if there is a risk of a brute force attack, the ML model can recommend the use of longer and more complex keys. By automating this process, ML can improve the efficiency and accuracy of cryptographic key swapping, ultimately enhancing the security of sensitive data.

There is a plethora of other avenues for how ML can integrate with PQC. This being said, there are important requirements to allow for the implementation of ML into a cryptographic ecosystem. On a large scale, the currently utilized cybersecurity ecosystem is insufficient to support an advanced cybersecurity system that is required for accepting and implementing ML. To face smarter, modern cyber attackers, our defenses must be able to be proactive and reactive based on attack patterns. More specifically, an advanced cybersecurity system is dependent on a more advanced software-based infrastructure. Likewise, a solution with proper key rotation cannot be implemented without having a system that is agnostic to which cryptographic key or algorithm it utilizes.

At the highest level, quantum computers are vast computational hardware improvements, while AI/ML provides seemingly limitless software potential. Combined, it is unimaginable what utility they can provide to an attacker. However, we can bolster the security of our devices by leveraging ML into our end-to-end encryption solutions. The thought leaders in the cybersecurity space are aware of the limitations of current encryption architecture and so are the attackers. If we want our cyber solutions to be smarter and protect our data from bad actors, we must implement a sophisticated, cutting-edge PQC system that leverages ML for good.

12.Prepare for quantum to fundamentally change PKI effectiveness

by John Cullen
https://www.computerweekly.com/opinion/Prepare-for-quantum-to-fundamentally-change-PKI-effectiveness

Encryption is a fundamental aspect of Public Key Infrastructure (PKI) – a service used to confirm identity by proving ownership of a private key. Encryption plays a crucial role in this process, ensuring the confidentiality and integrity of data to build confidence that senders and receivers of information are who they say they are.

However, the rise of quantum computing poses a significant threat to existing encryption protocols, potentially rendering them ineffective. Companies must be prepared for quantum to fundamentally change PKI effectiveness and explore the emerging field of post-quantum cryptography (PQC) as a solution to safeguarding data in the era of quantum technology.

The risks of quantum computing for PKI

Quantum computers work differently to that of conventional computers, and boast the ability to leverage quantum bits, or qubits, which can exist in multiple states simultaneously. This, effectively, allows them to take shortcuts to solve the hard mathematical problems that underpin current encryption systems.

Once large-scale, fault-tolerant quantum computers become a reality, encryption protocols that have protected sensitive information for years will become vulnerable to attacks. This is because cyber criminals, well-aware of these impending vulnerabilities, will eagerly exploit the weakness in PKI systems to gain unauthorised access to valuable data. It is therefore imperative for organisations to take proactive measures to protect themselves – before quantum technology becomes mainstream.

The consequences of PKI hacks extend beyond financial losses and immediate security breaches. When PKIs are compromised, hackers can achieve more privileged access, and once they have these "keys to the digital kingdom" they can wreak havoc – whether that's through manipulating company information or forcing service outages, for example. Compromised data confidentiality, identity theft, disruption of critical infrastructure, and erosion of trust pose severe risks not just to organisations, but to individuals and society as a whole. In fact, Statista's Cybersecurity outlook estimated the cost of cyber crime in 2022 was $8.44tn (£6.5tn), and this is expected to rise to $23.84tn by 2027.

Many organisations are already taking steps to protect their PKI. In fact, in a ranking of tech skills most in demand from ITJobsWatch, PKI jumped 240 places over the past year. However, these IT professionals need to think beyond well-known PKI protocols (such as not sharing privately hosted PKIs across communities with different security expectations) and take proactive steps to future-proof systems.

The future of a secure and connected world hinges on our ability to defend against PKI attacks and safeguard the trust we place in these – so the industry must explore new ways to bolster policies, procedures and technology.

Post-quantum cryptography: securing the future

Post-quantum cryptography (PQC) represents a revolutionary approach to encryption that aims to develop new cryptographic algorithms resistant to attacks by quantum computers. PQC seeks to provide mathematical problems that even quantum computers will find unsolvable, thereby ensuring the security of encrypted data.

PQC explores different mathematical frameworks, such as lattice-based, code-based, multivariate, and other novel cryptographic techniques. These algorithms are designed to withstand the immense computational power of quantum computers, making them a reliable solution for protecting sensitive information in the future.

PQC's benefits for PKI

By integrating PQC into PKI systems, organisations can fortify the security of critical national infrastructure, including transportation networks, energy grids, and vital communication channels. Additionally, the financial services sector, which heavily relies on secure transactions, can greatly benefit from PQC implementation.

Although PQC is still in its early stages, organisations and governments around the world are recognising the urgency of investing in this cutting-edge technology. The aim is to ensure that, as quantum computers pose a threat to the existing walls of encryption protecting data, PQC simultaneously constructs new, impregnable barriers.

The final word

As the advent of quantum computing looms closer, the future security of PKI hangs in the balance. The

risk of quantum attacks on existing encryption protocols demands proactive action from organisations and governments alike. Embracing post-quantum cryptography offers a promising solution to counteract these threats and ensure the long-term protection of sensitive data.

Four candidate cryptographic algorithms that aim to be quantum resilient have already been down-selected by NIST. There is, however, a risk that these candidate algorithms may not be sufficiently successful, so a hybrid model that leverages both post quantum and legacy RSA/ECC cryptographic algorithms is being used.

Investments in PQC research and development will pave the way for robust encryption algorithms that can withstand the computational prowess of quantum computers. By adopting PQC within PKI systems, critical sectors can enhance their resilience and maintain the integrity of their operations, safeguarding their sensitive information against the imminent threats posed by quantum technology.

Organisations must act now to stay ahead of the curve and actively prepare for the future of secure communication in the quantum era.

13.TII contributes to post-quantum cryptographic standardization via NIST digital signature schemes

https://www.zawya.com/en/press-release/companies-news/tii-contributes-to-post-quantum-cryptographic-standardization-via-nist-digital-signature-schemes-wyw3qtwy

The Technology Innovation Institute (TII), a leading global scientific research center and the applied research pillar of Abu Dhabi's Advanced Technology Research Council (ATRC), today announced that its Cryptography Research Center (CRC) has participated in a call for Additional Post-Quantum Digital Signature Schemes (DSS) issued by the American National Institute of Standards and Technologies (NIST). CRC has contributed to the submission of digital signature proposals in its continuing effort to help fortify and fast-track the evolution of post-quantum cryptographic (PQC) digital signatures.

The call for proposals is part of NIST's public process to define quantum-resistant public-key cryptography algorithms for standardization and diversify its portfolio of hard mathematical problems, based on structured lattices. NIST selected the first algorithms to be standardized in 2022, six years after the original public request for proposals to the PQC Standardization Process. NIST received 50 submissions in response and deemed 40 to be complete and admissible according to the submission requirements.

To provide the best proposals, TII collaborated with researchers of leading international partner universities across North America, Asia, and Europe to develop a cryptographic suite of DSS based on well-established hard mathematical problems. The schemes are based on a variety of mathematical problems that are believed to be resistant to quantum computers. The DSS suite includes MiRitH (MinRank Problem), PERK (Permutation Kernel Problem), RYDE (Rank Syndrome Decoding Problem), LESS (Code Equivalence Problem), MIRA (MinRank Problem), Biscuit (Multivariate Quadratic Problem), as well as SQISign (Quaternion Isogeny Path Problem).

Speaking on TII's participation in the prestigious initiative, Dr. Najwa Aaraj, Chief Researcher, Cryptography Research Center (CRC) said: "In line with our mission to discover breakthrough solutions to strengthen the future of digital societies, this contribution of several digital signatures to NIST under-

scores our commitment to advancing PQC. Such efforts enable us to realize our primary goal of addressing security challenges and to continuously push the boundaries of cryptographic research. Furthermore, our continuous strategic partnerships with globally-renowned universities are a testament to our collaborative spirit and help redefine the cryptography landscape and ensure secure communication for a connected world."

TII's active participation in augmenting the PQC ecosystem demonstrates its expertise in the field and highlights the importance of academic synergies in establishing a holistic approach to drive secure and robust cryptographic solutions.

14.Quantum Cryptography: The Future of Secure Digital Payments

by Liam Critchey
https://www.electropages.com/blog/2023/07/future-digital-payments-deep-dive-quantum-cryptography

Digital payments and digital banking have become more and more popular over the last decade or so and have replaced cash transactions in many parts of society. The adoption of online banking and digital payments was also accelerated during the COVID-19 pandemic when most transactions involved no cash at all in preventing viral transmission.

While physical money is not obsolete, it is less commonly used in many parts of the world (especially the Western world). If society is to switch to digital payments being the main way of paying, then they need to have a similar level of security as physical payments—especially being tamper-resistant and untraceable. However, digital payments also need an extra layer of security because, unlike physical notes, digital payments are susceptible to digital attackers and data breaches, so digital payment providers need to be more vigilant in the prevention of cyberattacks.

Recent advancements in quantum technologies have shown great potential in enhancing the security of digital transactions. Quantum cryptography, for instance, offers a level of security that is theoretically unbreakable, making it an attractive solution for securing digital payments.

Current Security Measures in Digital Payment

Current digital payment technology is already encrypted. In today's transactions, the sensitive banking data inputted by a customer is turned into random tokens and the unique sequence is secured with a cryptographic function called a cryptogram. However, as many will know, banking data is just as privy to data breaches and cyber-attacks if a high enough computational power is used.

Like many areas of cybersecurity today, quantum technologies have the potential to create a more secure communication channel between two user points. Quantum communication channels have the potential to protect digital transaction channels by a much greater degree than classical methods, even against attacks with infinite computational power.

Turning Towards Quantum Cryptography

Quantum cryptography has been a rapidly growing area of interest when it comes to both the cybersecurity and quantum technology fields, with the potential for quantum channels to run alongside classical communication channels and provide an enhanced level of security. Current classical cryptography sys-

tems rely on computationally hard mathematical problems, but it's possible to replace these with new quantum systems that are resistant to high-powered computational attacks—as a high computational power can still break through these classic computational problems if enough computational power is used.

The Quantum Communications Hub, a major collaboration of university and industrial partners funded through the UK National Quantum Technologies Programme is accelerating the development and commercialisation of quantum secure communications technologies. This includes Quantum Key Distribution (QKD), a mature quantum technology that enables ultra-secure distribution of encryption keys.

There have been some developments in the field so far that use quantum technology to provide an extra layer of security. However, with the development of quantum algorithms comes the good and the bad, so while quantum algorithms can be used as a protection against cyberattacks, they could also be used to perform an attack as they can have a much higher degree of computational power than classical algorithms. So new cryptographic systems also need to be resistant to quantum attacks as well, and while a number of potential solutions have been developed to some degree, some of them are still privy to being broken by high-powered computational attacks.

Quantum Key Distribution (QKD) the Conventional Choice for Trusted Parties

Quantum mechanical laws can provide an added layer of security against high-powered computational attacks. The general field of information security is growing, with quantum key distribution (QKD) being the most widely matured and implemented quantum technology today. QKD allows to trusted parties to communicate over a public channel without the fear of the data being intercepted by classical computational attacks.

QKD uses a quantum channel alongside a classical channel, where a secure key (a randomly distributed number sequence) is generated from the random polarisation of photons. In QKD, both the classical and quantum channels generate a sequence, but the data is held in the quantum channel. So, if a hack takes place in the classical channel, the users can see that an attack was attempted (as there will be an imperfection in the signals), but no data can be obtained. QKDs have been growing in use for communications between trusted parties, and it's now possible to secure connections over 500 km when using optical fibres and 1000 km when using satellites.

However, most digital payments nowadays are not made between two trusted parties, and most payments are usually between a customer and a merchant. This can take the form of contactless purchases between in-person interactions between a merchant and a customer or through an online banking purchase. This brings its own set of challenges when trying to integrate quantum-based security systems as these digital payments are susceptible to attack from external hackers (or from a direct malicious transaction due to unscrupulous merchants), but QKD is not a suitable cryptography method in these instances.

For transactions of this nature, there needs to be a binding commitment between the customer, the merchant, and the bank (or the payment provider if it's a third party) to guarantee that the transaction is valid. This is typically done using a cryptogram, which uses a hash function to guarantee a one-time purchase. However, because not all the parties are trusted in merchant-customer purchases, QKD cannot be used to provide a guarantee on the validity of the transaction because the cryptogram (which is the classical output) is handled by the untrusted parties themselves—rendering the safety of the communication useless if the merchant is the one who is the perpetrator of the malicious transaction. So, for these types of digital transactions, other quantum technologies are being sought to provide a greater degree of security.

Quantum Light Could offer A Solution for Untrusted Parties

There have been a number of investigations into using quantum light in the banking space. Previous studies have looked at using quantum light to prevent banknote counterfeiting, as well as preventing double spending with either tokens or credit cards. However, introducing these concepts into everyday spending scenarios is no easy task because the quantum states need to be stored across much longer time periods—such as days or months—to ensure that users can spend flexibly using their normal, everyday habits. Unfortunately, the required time frames are well beyond what is possible with quantum storage operations today—which range from a few microseconds to a few minutes.

While quantum storage is not feasible, quantum light can provide a number of practical security advantages compared to classical methods for everyday payments. Researchers have now used quantum light to guarantee a one-time purchase. Like classical payments, the system involves a customer, a merchant, and a bank/credit card institute.

In this system, none of the classical or quantum communication channels are deemed to be trusted other than an initial step between the customer and the bank that is required to create an account. Other than the bank, it is assumed that any of the other parties could act maliciously.

When a payment is made, the bank sends a set of quantum states (in the form of quantum light) to the customer's device. The device then measures the quantum states and converts them into a quantum-secured token, i.e., a quantum cryptogram. The customer then uses this token to pay the merchant, and the merchant contacts the bank for payment verification. If it's accepted, then the money is transferred by the bank from the customer's account to the merchant's account.

Advantages and Challenges of Quantum Light-Based Payment Systems

In this quantum payment process, the cheating probability is very low and is resistant to noise and loss-dependent attacks. For the customer, the implementation of such a quantum system does not require any challenging technology implementation other than single-photon detection. The sensitive information belonging to the customer is guaranteed to be sealed, and no cross-communication protocols are required to validate a transaction when multiple verifier branches are involved.

Additionally, any feasible payment system must be able to reject payments without compromising the sensitive data of the customer. In this system, the payment is sent over the quantum channel and the cryptogram over the classical channel. If the cryptogram comes back malformed, then the payment will be rejected. This behaves in a similar way to QKD, where the quantum channel transmits the sensitive data and the classical channel checks for any malicious intent (in this case, a malicious payment or a hack in the case of QKD).

The current system does have longer than ideal communication time in its current state (this can be rectified with stronger light sources), but it presents an opportunity to develop a new quantum cryptographic system that can be used with untrustworthy parties. This approach does not hinge on long-term quantum storage or the use of trusted agents and authenticated channels, so it could be more accessible for everyday payments compared to other quantum cryptography methods.

The Quantum Communications Hub and Its Contributions to Quantum Secure Communications

The Quantum Communications Hub, a major collaboration of university and industrial partners, has been instrumental in accelerating the development and commercialisation of quantum secure communications technologies. Some of their notable achievements include the creation of the UK's first Quantum Network, the miniaturisation of QKD technologies, and the demonstration of free-space QKD between handheld devices.

Their vision for the future includes extending the UK Quantum Network, further miniaturising QKD technologies, overcoming distance limitations of terrestrial fibre-based QKD, and developing new quantum

sources, detectors, and protocols beyond QKD.

The University of Oxford is working on the development of miniature, reliable, low-cost, handheld QKD systems. These systems have the potential to provide future contactless payment methods and a wide range of other applications. They are also working on combining fibre QKD with free-space QKD to create secure wireless systems that could be used in next-generation mobile networks.

Conclusion: The Future of Quantum Secure Payments

The evolution of digital payments is moving at a rapid pace, and the integration of quantum technologies presents a promising path towards enhanced security. Quantum cryptography, particularly Quantum Key Distribution (QKD), has already shown its potential in securing communications between trusted parties. However, the challenge lies in adapting these technologies for transactions involving untrusted parties, which constitute a significant portion of digital payments today.

The use of quantum light in digital payments is a promising development that could overcome some of these challenges. While there are still hurdles to overcome, such as the need for long-term quantum storage and the development of more robust light sources, the potential benefits are significant. The ability to guarantee one-time purchases and protect sensitive customer data, even in the presence of potentially malicious parties, could revolutionise the security of digital transactions.

With ongoing research and development in institutions such as the Quantum Communications Hub at the University of Oxford, the future of quantum secure payments looks promising. As these technologies continue to mature, they could potentially become a standard feature of digital transactions, providing an unprecedented level of security and trust in the digital payment landscape[2].

15.Controlling Quantum Randomness From the Vacuum

by Matt Swayne
https://thequantuminsider.com/2023/07/14/controlling-quantum-randomness-from-the-vacuum/

A team of researchers from the Massachusetts Institute of Technology has achieved a milestone in quantum technologies, demonstrating for the first time the control of quantum randomness.

The team of researchers focused on a unique feature of quantum physics known as “vacuum fluctuations”. You might think of a vacuum as a completely empty space without matter or light. However, in the quantum world, even this “empty” space experiences fluctuations or changes.

Imagine a calm sea that suddenly gets waves – that’s similar to what happens in a vacuum at the quantum level. Previously, these fluctuations have allowed scientists to generate random numbers. They’re also responsible for many fascinating phenomena that quantum scientists have discovered over the past hundred years.

The findings are described today in the journal Science, in a paper lead by MIT postdoctoral associates Charles Roques-Carmes and Yannick Salamin; MIT professors Marin Soljacic and John Joannopoulos; and co-workers.

Conventionally, computers function in a deterministic manner, executing step-by-step instructions that

follow a set of predefined rules and algorithms. In this paradigm, if you run the same operation multiple times, you always get the exact same outcome. This deterministic approach has powered our digital age, but it has its limitations, especially when it comes to simulating the physical world or optimizing complex systems, tasks that often involve vast amounts of uncertainty and randomness.

This is where the concept of probabilistic computing comes into play. Probabilistic computing systems leverage the intrinsic randomness of certain processes to perform computations. They don't just provide a single "right" answer, but rather a range of possible outcomes each with its associated probability. This inherently makes them well-suited to simulate physical phenomena and tackle optimization problems where multiple solutions could exist and where exploration of various possibilities can lead to a better solution. However, the practical implementation of probabilistic computing has been hampered historically by a significant obstacle: the lack of control over the probability distributions associated with quantum randomness. But the research conducted by the MIT team has shed light on a possible solution.

Specifically, the researchers have shown that injecting a weak laser "bias" into an optical parametric oscillator, an optical system that naturally generates random numbers, can serve as a controllable source of "biased" quantum randomness.

"Despite extensive study of these quantum systems, the influence of a very weak bias field was unexplored," remarks Charles Roques-Carmes, a researcher in the study. "Our discovery of controllable quantum randomness not only allows us to revisit decades-old concepts in quantum optics but also opens up potential in probabilistic computing and ultra-precise field sensing."

The team has successfully exhibited the ability to manipulate the probabilities associated with the output states of an optical parametric oscillator, thereby creating the first-ever controllable photonic probabilistic bit (p-bit). Additionally, the system has shown sensitivity to the temporal oscillations of bias field pulses, even far below the single photon level.

Yannick Salamin, another team member, remarks, "Our photonic p-bit generation system currently allows for the production of 10,000 bits per second, each of which can follow an arbitrary binomial distribution. We expect that this technology will evolve in the next few years, leading to higher-rate photonic p-bits and a broader range of applications."

Professor Marin Soljacic from MIT emphasizes the broader implications of the work: "By making the vacuum fluctuations a controllable element, we are pushing the boundaries of what's possible in quantum-enhanced probabilistic computing. The prospect of simulating complex dynamics in areas such as combinatorial optimization and lattice quantum chromodynamics simulations is very exciting."

16.Quantum Technology — Advancing Applications in Space

by Daniel Mathews
https://medium.com/@danielmathews4002/quantum-technology-advancing-applications-in-space-7ef607f21582

On the 14th of July at 2.35 PM IST, all eyes were on Satish Dhawan Space Centre in Sriharikota as the ISRO launched the Chandrayaan-3 mission, kick-starting a forty-day journey to the moon! This significant achievement demonstrates India unwavering commitment of making its mark in space.

Forbes published an article in December 2022, stating that space could play a key role in advancing quantum innovation, in three ways. Firstly, space provides extremely cold temperatures which are required for quantum computers, but are expensive to replicate on earth. Secondly, space offers an interference-free controlled environment which again would be expensive and difficult to achieve on earth. Thirdly, in space, there is a free flow of information thus the need for extensive physical data pipelines doesn't arise. Although quantum technology is still far from being perfect there is significant progress happening in different parts of the world.

In March 2023, in collaboration with ISRO, the Quantum Information and Computing Lab of Raman Research Institute in Bengaluru, made a breakthrough in secure quantum communication using satellites. Harnessing the power of Quantum Key Distribution, they were able to demonstrate secure communication between a moving receiver and a stationary device, using a Pointing, Acquisition and Tracking system.

In April 2023, in collaboration with Accenture, post-quantum security leader QuSecure carried out a successful test for multi-orbit data communications using post-quantum cryptography, delivering a quantum-resilient crypto-agile channel from Earth to LEO (low earth orbit) and then to a GEO (geosynchronous orbit) satellite and back to Earth. Leveraging both quantum-resilient cybersecurity and classical cybersecurity, the transmission was secured using QuSecure's QuProtect platform.

In May 2023, the European Space Agency selected Thales Alenia Space, a Franco-Italian company for its TeQuantS project, which stands for Technological development for space-based Quantum reSource Distribution. One of the objectives of this project, which is proposed to go live in 2035, would be to build two optical ground stations that would be linked from a satellite through a long-distance quantum communications link.

Just three days ago, it was reported that the UK Space Agency has partly funded researchers at the University of Strathclyde who have partnered with the University of Bristol to develop robust, low-power, compact sources for satellite quantum key distribution using new advances in the ultraviolet micro-LEDs. It will seek to address current issues with laser diodes in satellite quantum key distribution sources such as the requirement for thermal control and fluctuations in intensity.

While quantum technology is slowly but surely leaving its mark on industries such as healthcare and finance, its applications in space are becoming more evident. From the possibility of quickly and accurately analyzing vast amounts of space images, measurements and other data to running complex simulations and securing communications in space, the future is indeed looking bright!

17.Hardware security entering quantum computing era

by Majeed Ahmad
https://www.edn.com/hardware-security-entering-quantum-computing-era/

A new IP offering post quantum cryptography (PQC) hardware security is now available for chip and system providers to secure data center and artificial intelligence (AI) workloads. The Quantum Safe security IP unveiled by Rambus aims to safeguard data centers and advanced workloads like generative AI against quantum attacks.

Quantum computers will be able to rapidly break current asymmetric encryption, so the National Institute

of Standards and Technology (NIST) has been busy identifying post-quantum cryptographic algorithms since 2016. According to Heather West, research manager of Quantum Computing Research at IDC, these algorithms will be better suited for protecting critical government and public infrastructure from entities looking to steal data now to decrypt later using quantum computing.

Next, the NIST announced its first four post-quantum computing recommendations, which means system designers can start implementing quantum-resistant cryptography. Quantum Safe IP from Rambus is an effort to provide the root of trust for data center and communications security in the quantum computing era.

The company's root of trust IP uses the two quantum-compute resistant cryptographic algorithms selected by the NIST: CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures.

The security IP also supports the Commercial National Security Algorithm Suite (CNSA) algorithms for software and firmware updates, including XMSS/LMS stateful hash firmware signatures, CNSA symmetric-key algorithms, and CNSA quantum-resistant public-key algorithms.

Rambus' root of trust security solution features a programmable 32-bit secure processor and supports Open Compute Project (OCP) Caliptra root of trust for measurement with DICE and X.509. It also features true random number generator (TRNG) and physical unclonable function (PUF) entropy source.

Quantum Safe security IP comes with a software development kit (SDK) for user development of secure and trusted applications.

18.White House publishes National Cybersecurity Strategy Implementation Plan

https://www.helpnetsecurity.com/2023/07/13/national-cybersecurity-strategy-implementation-plan-published/

The Biden-Harris Administration's recently released National Cybersecurity Strategy calls for two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace:

- **Ensuring that the biggest, most capable, and best-positioned entities** – in the public and private sectors – assume a greater share of the burden for mitigating cyber risk
- **Increasing incentives to favour long-term investments into cybersecurity**

Today, the Administration is announcing a roadmap to realize this vision. It is taking the novel step of publishing the National Cybersecurity Strategy Implementation Plan (NCSIP) to ensure transparency and a continued path for coordination. This plan details more than 65 high-impact Federal initiatives, from protecting American jobs by combatting cybercrimes to building a skilled cyber workforce equipped to excel in our increasingly digital economy.

The NCSIP, along with the Bipartisan Infrastructure Law, CHIPS and Science Act, Inflation Reduction Act, and other major Administration initiatives, will protect investments in rebuilding America's infrastructure, developing our clean energy sector, and re-shoring America's technology and manufacturing base.

Each NCSIP initiative is assigned to a responsible agency and has a timeline for completion. Some initiatives, such as the issuance of the Administration's Cybersecurity Priorities for the Fiscal Year 2025 Budget, have been completed ahead of schedule. Other completed activities, such as the transmittal of the May 26th Department of Defense 2023 Cyber Strategy to Congress, and the June 20th creation of a new National Security Cyber Section by the Justice Department, are key milestones in completing initiatives. This is the first iteration of the plan, which is a living document that will be updated annually.

Eighteen agencies are leading initiatives in this whole-of-government plan demonstrating the Administration's deep commitment to a more resilient, equitable, and defensible cyberspace. The Office of the National Cyber Director (ONCD) will coordinate activities under the plan, including an annual report to the President and Congress on the status of implementation, and partner with the Office of Management and Budget (OMB) to ensure funding proposals in the President's Budget Request are aligned with NCSIP initiatives.

The Administration looks forward to implementing this plan in continued collaboration with the private sector, civil society, international partners, Congress, and state, local, Tribal, and territorial governments. As an example of the Administration's commitment to public-private collaboration, ONCD is also working on a request for information regarding cybersecurity regulatory harmonization that will be published in the near future.

The NCSIP is not intended to capture all Federal agency activities in support of the NCS. The following are sample initiatives from the plan, which is organized by the NCS pillars and strategic objectives.

Pillar one: Defending critical infrastructure

Update the National Cyber Incident Response Plan (1.4.1): During a cyber incident, it is critical that the government acts in a coordinated manner and that private sector and SLTT partners know how to get help. The Cybersecurity and Infrastructure Security Agency (CISA) will lead a process to update the National Cyber Incident Response Plan to more fully realize the policy that "a call to one is a call to all." The update will also include clear guidance to external partners on the roles and capabilities of Federal agencies in incident response and recovery.

Pillar two: Disrupting and dismantling threat actors

Combat Ransomware (2.5.2 and 2.5.4): Through the Joint Ransomware Task Force, which is co-chaired by CISA and the FBI, the Administration will continue its campaign to combat ransomware and other cybercrime. The FBI will work with Federal, international, and private sector partners to carry out disruption operations against the ransomware ecosystem, including virtual asset providers that enable laundering of ransomware proceeds and web fora offering initial access credentials or other material support for ransomware activities.

A complementary initiative, led by CISA, will include offering resources such as training, cybersecurity services, technical assessments, pre-attack planning, and incident response to high-risk targets of ransomware, like hospitals and schools, to make them less likely to be affected and to reduce the scale and duration of impacts if they are attacked.

Pillar three: Shaping market forces and driving security and resilience

Software Bill of Materials (3.3.2): Increasing software transparency allows market actors to better understand their supply chain risk and to hold their vendors accountable for secure development practices. CISA continues to lead work with key stakeholders to identify and reduce gaps in software bill of materials (SBOM) scale and implementation. CISA will also explore requirements for a globally-accessible database for end of life/end of support software and convene an international staff-level working group

on SBOM.

Pillar four: Investing in a resilient future

Drive Key Cybersecurity Standards (4.1.3, 4.3.3): Technical standards are foundational to the Internet, and U.S. leadership in this area is essential to the vibrancy and security of cyberspace. Consistent with the National Standards Strategy, the National Institute of Standards and Technology (NIST) will convene the Interagency International Cybersecurity Standardization Working Group to coordinate major issues in international cybersecurity standardization and enhance U.S. federal agency participation in the process. NIST will also finish standardization of one or more quantum-resistant publickey cryptographic algorithms.

Pillar five: Forging international partnerships to pursue shared goals

International Cyberspace and Digital Policy Strategy (5.1.1 and 5.1.2): Cyberspace is inherently global, and policy solutions must reflect close collaboration with our partners and allies. The Department of State will publish an International Cyberspace and Digital Policy Strategy that incorporates bilateral and multilateral activities. State will also work to catalyze the development of staff knowledge and skills related to cyberspace and digital policy that can be used to establish and strengthen country and regional interagency cyber teams to facilitate coordination with partner nations.

19.Japanese Banking Giant Makes Strategic Quantum Investment

by Matt Swayne
https://thequantuminsider.com/2023/07/13/japanese-banking-giant-makes-strategic-quantum-investment/

MUFG Bank, one of Japan's largest financial institutions, has made a strategic investment in Groovenauts, a Japanese startup specializing in quantum computer technology, according to Nikkei.

This move could signal MUFG's determination to leverage quantum technology to enhance its financial services, including complex transactions like derivatives trading and asset risk management, while also improving operational efficiency, the financial news service reported.

Groovenauts employs a method known as quantum annealing. By using this approach, the company can find optimal solutions from an extensive range of combinations. Groovenauts connects quantum computers owned by research institutes with companies that want to use them, as reported by Nikkei. Through a combination of data processing technology and artificial intelligence, the company makes it easier to use quantum computers for business and other purposes, according to the financial news service.

MUFG Bank is aiming to gain an early advantage in the race to acquire quantum technology by investing in Groovenauts, Nikkei reported.

As part of the investment, MUFG Bank has purchased 18% of Groovenauts' outstanding shares, amounting to several billion yen, Nikkei reports. This equity-method affiliation marks the first direct investment in a quantum computing startup by any of the three Japanese megabanks, the financial service added. MUFG Bank will also appoint a board member to the startup, according t0 Nikkei.

The bank's primary objective in embracing quantum technology is to mitigate the risks associated with financial derivatives transactions, Nikkei reported. MUFG is also exploring the potential of using quantum technology alongside interactive AI systems, according to the financial news service.

Preliminary tests conducted by MUFG Bank have shown promising results, indicating that tasks currently taking an hour to complete can be accomplished in a matter of seconds with the aid of quantum computers, Nikkei reported. The bank intends to introduce this technology into practical applications as early as fiscal year 2024, focusing on areas that present the greatest opportunities.

The bank's investment marks another milestone for Japan, which is rapidly making headway to become a global quantum leader. Several prominent Japanese companies, including Toyota Motor, Sony Group, JSR and Mitsubishi Chemical Group, are exploring the integration of quantum computers into their operations, according to Nikkei. In the financial sector, Mizuho Financial Group and Sumitomo Mitsui Financial Group are actively researching the utilization of quantum technology, reported Nikkei.

MUFG Bank has been on a proactive trajectory of technology acquisition through investments in both domestic and international tech companies, Nikkei reported. The bank's recent investment in Groovenauts follows its plans to acquire Kanmu, a Japanese startup specializing in deferred payment services, and its investment in an Israeli fintech company that utilizes AI technology to provide loans.

With its strategic investment in Groovenauts, MUFG Bank has positioned itself at the forefront of the quantum computing revolution in the financial industry, according to Nikkei.

20.Internet Engineering Task Force standardises quantum-safe VPN protocol created by Post-Quantum

by Eastern Daylight Time
https://www.businesswire.com/news/home/20230713587680/en/Internet-Engineering-Task-Force-standardises-quantum-safe-VPN-protocol-created-by-Post-Quantum

The world's efforts to secure digital communications from the threat posed by quantum computers took a significant leap forward today as a new standard for quantum-safe Virtual Private Networks (VPN) was ratified by the Internet Engineering Task Force (IETF).

The new protocol has already been used by Banque de France and Deutsche Bundesbank to secure payments messages, paving the way for full adoption by the Bank for International Settlements to secure communications between the world's central banks.

'Harvest Now Decrypt Later' (HNDL) attacks currently represent the greatest quantum cybersecurity threat. These attacks see hostile actors steal encrypted data now which can be decrypted once a sufficiently mature quantum computer comes online. The new US Quantum Computing Cybersecurity Preparedness Act states that the HNDL risk presents the highest threat to humankind and stipulates that quantum migration must start now. Deploying a VPN based on new post quantum cryptography is the easiest way to protect data-in-transit from such attacks.

The new IETF standard specifies how VPNs can exchange communications securely in the quantum age. The novel approach prioritises interoperability by making it possible for multiple post-quantum and classical encryption algorithms to be incorporated into VPNs. Combining both old and new encryption is essential to ensure no disruption to the functioning of existing IT systems, and to protect data from attack by both classical and quantum computers.

This is a particularly important milestone for internet connectivity and security as we are transitioning from an era where the world relied upon just one or two algorithms (RSA and Elliptic Curve), to a situation where different nation states are deploying a wide variety of different post-quantum algorithms. This new IETF standard is the glue that allows parties using different public key encryption algorithms to talk with one another.

The new IETF standard was proposed and designed by Post-Quantum, a British cyber security company that's built a portfolio of market-ready quantum-safe cyber security products. Post-Quantum's own Hybrid PQ VPN uses the new IETF standard and is already in use by NATO to secure its communications from quantum attack, supporting interoperable communications between NATO members.

CJ Tjhai, CTO, Post-Quantum and original author of the new IETF standard said: "I'd like to thank all the technologists that collaborated with us on this IETF standard. Much of the focus has been on NIST's new post quantum encryption algorithms themselves, but this is insufficient unless you have a protocol that defines how the connectivity is done. The easiest way to prevent Harvest Now Decrypt Later attacks is to deploy a PQ VPN based on the new IETF standard. NIST's new algorithms are only useful if we have agreed standards for their use and mature products that can accommodate them."

Andersen Cheng, Executive Chairman, Post-Quantum added: "CJ and his collaborators have completed important work that makes it possible for tech companies to build quantum-safe VPNs that communicate to one another. We are entering a period where different countries are now recommending different encryption algorithms, so engineering our communications infrastructure to be interoperable and backward compatible is absolutely crucial. That's the value our own VPN is bringing to organisations like NATO, a diverse member organisation with a variety of post-quantum algorithms in use.

"In the commercial sector, we are pleased that Banque de France and Deutsche Bundesbank have also recently completed their project in transmitting payment messages using our protocol, which will pave the way for the Bank for International Settlements to build a complete chain of trust for central bank applications to counter any HNDL risks they already face today."

José María Lucía Moreno, Lead Partner, EY Wavespace and a Post-Quantum partner added: "Our agreement with Post-Quantum is an important step in helping EY and its clients to become quantum-safe. We're increasingly consulting with our clients to identify where they use traditional encryption that will need to be upgraded, and to help them prepare for the quantum era. Post-Quantum's approach is particularly interesting because they have modular software-based products like the VPN, which can be implemented together, or as standalones within existing environments, to offer protection today."

21.Chinese hackers forged authentication tokens to breach government emails

by Zeljka Zorz
https://www.helpnetsecurity.com/2023/07/12/storm-0558-forged-authentication-tokens/

Sophisticated hackers have accessed email accounts of organizations and government agencies via authentication tokens they forged by using an acquired Microsoft account (MSA) consumer signing key, the company has revealed on Tuesday.

"The threat actor Microsoft links to this incident is an adversary based in China that Microsoft calls **Storm-0558**. We assess this adversary is focused on espionage, such as gaining access to email systems for intelligence collection."

This specific hacking group primarily targets government agencies in Western Europe, the company added. But according to The Washington Post, these latest attacks also compromised a number of unclassified U.S. email accounts.

The hackers exploited a token validation issue

Microsoft began investigating anomalous mail activity on June 16, 2023, after being alerted by customers.

They ultimately established that the account compromises started the day before, and that the attackers managed to access email accounts of employees at 25 organizations and some consumer accounts of individuals associated with those organizations.

The attackers gained access via Outlook Web Access in Exchange Online (OWA) and Outlook.com.

"MSA (consumer) keys and Azure AD (enterprise) keys are issued and managed from separate systems and should only be valid for their respective systems. The actor exploited a token validation issue to impersonate Azure AD users and gain access to enterprise mail," Microsoft explained.

"We have no indications that Azure AD keys or any other MSA keys were used by this actor. OWA and Outlook.com are the only services where we have observed the actor using tokens forged with the acquired MSA key."

Microsoft says customers don't have to do anything to protect themselves against this attack – the company has implemented mitigations (blocked the usage of maliciously signed tokens issued with the key and replaced it). There is no mention of them fixing the exploited token validation issue, though.

All targeted or compromised organizations have been contacted by Microsoft directly via their tenant admins and and have been provided with information to help them investigate and respond. "If you have not been contacted, our investigations indicate that you have not been impacted," the company added, and promised to share "new details and recommendations as appropriate."

Microsoft has also shared on Tuesday that attackers have been exploiting its Microsoft Windows Hardware Developer Program (MWHDP) to sign malicious drivers, and has released fixes for various zero-days actively exploited in the wild.

UPDATE (June 1, 2023, 04:40 a.m. ET):

As it turns out, the attacks were spotted by a US Federal Civilian Executive Branch agency, when they detected suspicious log events.

"In Mid-June 2023, an FCEB agency observed **MailItemsAccessed** events with an unexpected **ClientAppID** and **AppID** in M365 Audit Logs. The **MailItemsAccessed** event is generated when licensed users access items in Exchange Online mailboxes using any connectivity protocol from any client. The FCEB agency deemed this activity suspicious because the observed **AppId** did not normally access mailbox items in their environment. The agency reported the activity to Microsoft and CISA," the CISA

and the FBI said in a cybersecurity advisory released on Wednesday.

"The affected FCEB agency identified suspicious activity by leveraging enhanced logging—specifically of **MailItemsAccessed** events — and an established baseline of normal Outlook activity (e.g., expected **AppID**). The **MailItemsAccessed** event enables detection of otherwise difficult to detect adversarial activity."

They advised agencies and critical infrastructure organizations to enhance monitoring in Microsoft Exchange Online environments by implementing the logging recommendations outlined in the advisory.

UPDATE (July 14, 2023, 15:10 a.m. ET):

Microsoft has shared more in-depth details about the attack, but the company still hasn't discovered how the threat actor acquired the MSA consumer signing key.

"Though the key was intended only for MSA accounts, a validation issue allowed this key to be trusted for signing Azure AD tokens. This issue has been corrected," Microsoft says.

22.Preparing businesses' digital trust for a post-quantum world

by Armando Dacal
https://itbrief.com.au/story/preparing-businesses-digital-trust-for-a-post-quantum-world

As governments map a path toward next-generation cryptography, businesses must take steps today to ensure the integrity of their most important data before quantum decryption opens the door to all of today's secrets.

In recent months, there has been a welcome acceleration in government planning for a post-quantum world. The Australian federal government launched the National Quantum Strategy in May, which clearly states the three key categories of quantum technology as it impacts our future: quantum sensing, quantum computers, and quantum communications.

While there are many elements of quantum technology that sit on a long horizon, it feels important for every business to understand, as soon as possible, what will change when stable quantum computing arrives. Within quantum computation lies the age of post-quantum cryptography, and whether your business directly deploys quantum computers or not, it will bring fundamental change to the nature of cybersecurity.

We have probably all heard the core concept – today's most powerful encryption algorithms will soon see a day when an adversary has the power to break the key in minutes or even seconds. This is a Y2K tier concern, with even more certainty that the crisis will have real impact but little certainty on when exactly it could be. Ten years? Five years? One year?

What we do know is that motivated adversaries with nation-state-level resources will be eager to be the first to achieve this level of quantum technology. Once it is available, there will be those who intend to use it both in real-time online and to decrypt stolen data they have held for some time but have not yet been able to crack.

In the absence of direct solutions today, enterprise security should be building as much visibility as possible on its specific cryptographic trust profile. Like so many other areas of technology, we cannot build a clear roadmap for something we haven't measured. For digital trust in our modern, connected world, that means building an inventory of the certificates that underpin every secure digital asset and communication protocol. It involves having the crypto agility in place to be able to seamlessly find and replace encrypted assets with updated ones when necessary.

We know that the average large business has thousands of certificates, with global-scale enterprises holding into the tens of millions across an organisation. But how many know exactly where they all are and analyse them for potential risk factors?

Through tools like our own DigiCert Trust Lifecycle Manager, any organisation can identify and manage its certificates and PKI services in a centralised way. This is an essential step toward knowing where all your digital assets lie, what algorithms are being used to protect them, how your certificates are currently managed, and when they expire.

By creating an inventory, it becomes possible to prioritise for a post-quantum future. Which digital assets are your most important for long-term protection? What is most at risk? We know that asymmetric algorithms like RSA and ECC are under threat, while symmetric keys like AES-256 look to be quantum-safe. Across our networks, services and devices, we can build an understanding of where we need enhanced protection and how to prioritise our most critical assets.

How do you ensure your most valuable secrets are hard to find in a world without locks? We can consider these questions today to put plans in place before quantum-safe algorithms are a must and before it is too late.

As an industry, we need to continue to build our understanding of the change that is to come and to know what it means to be as prepared as possible. For our part, DigiCert is working closely with industry and government agencies, like the National Institute for Science and Technology in the USA on defining next-generation standards that will deliver the protection we need in that post-quantum era.

Ideally, we will have new solutions in place ahead of the quantum technology being available. But today's standards have been built over the course of the past two decades, so while there is cause to move quickly, every new standard needs to be carefully considered and rolled out to ensure we get it right – especially given the stakes of a post-quantum era.

We know there's a lot on the plate of CIOs and CSOs today. But achieving visibility as your starting point to building plans for the next era of cybersecurity should become an important tool in your arsenal when questions begin to land from the board on whether you have taken any steps to understand your organization's readiness for a post-quantum future.

23.Unbreakable communications using the power of quantum cryptography

by Andrey Feldman
https://www.advancedsciencenews.com/unbreakable-communications-using-the-power-of-quantum-cryptography/

In recent years, secure and hack-proof communications have become increasingly important in industry,

economics, politics, and even private activities. However, traditional ways of encrypting data are rapidly losing their reliability due to the development of quantum computers, which are able to decrypt encoded information orders of magnitude faster than their classical counterparts, posing a significant challenge.

The answer to this "quantum threat" has been the development of encryption methods based on the fundamental principles of quantum mechanics. One such technique is quantum key distribution, where two parties share a secret key known only to them. The key can be used to encrypt and decrypt messages transmitted over classical communication channels, such as broadcasting, television, or the internet.

"Quantum key distribution is a secured way to transmit a key between a sender and a receiver," explained Igor Aharonovich, a professor in the School of Mathematical and Physical Sciences at the University of Technology Sydney, in an email.

"Information is encoded in individual particles of light (single photons)," he continued. "What makes it secure is the fact that you cannot clone a single photon, hence if the channel is eavesdropped, it will be immediately detected. Quantum key distribution is important because it is the only way to ensure an absolutely secured connection protected by law of quantum physics."

Finding a sufficient source

A third party's inability to clone a particle whose state carries an information about the key stems from the fact that it is impossible to interact or measure a quantum particle without changing its state. For example, this could be a photon whose polarization exists in a specific state, which is the quantum equivalent to an elementary particle's spin state. Any interaction with the photon used as the key would introduce anomalies in the transmitted signal that the communicating parties can easily detect.

For quantum key distribution to work reliably, it is crucial that photon source emit only one photon at a time. If the source accidentally emits two or more photons in the same state, it creates an opportunity for an eavesdropper to manipulate one of them without changing the state of the others, potentially obtaining information about the key that would go unnoticed by the communicating parties.

"The main challenge [to implementing quantum key distribution] is to find a sufficiently bright source of single photons," said Aharonovich. "Since the communication is done by photons, you need a source that would emit those photons fast."

In 2022, researchers proposed using a graphene-like crystalline compound called hexagonal boron nitride as such a photon source, because introduced defects in its crystal lattice can result in the emission of single photons with well-controlled polarization when irradiated with a laser.

Based on the results of this study, Aharonovich and his colleagues were able to implement a hexagonal boron nitride-based quantum key distribution protocol in practice, reported in a recent paper published in *Advanced Quantum Technologies*.

Putting quantum keys into practice

The team built an apparatus in which the sender and receiver of an encrypted signal were located at a distance of only a few tens of centimeters from each other. The sender could generate hundreds of thousands of photons per second, each carrying one bit of information about the quantum key.

One of the key features of their installation is that due to the unique physical properties of hexagonal boron nitride as the photon source it can operate at room temperature, distinguishing it from many alternative devices, which require cryogenic temperature to reliably generate single photons in well-controlled states. Crucially, all the components of their apparatus, such as polarizers and signal amplifiers,

are affordable and commercially available.

“The key novelty of our work is the implementation of the fastest and purest source of single photons at room temperature,” said Aharonovich, summing up the significance of the study. “We then attempted quantum key distribution and demonstrated an absolutely secured transmission.”

As proof-of-concept, the researchers encoded an image of a toy car, transmitted it using their machine, and subsequently decoded, obtaining a perfect match between the original and received images.

The scientists expect that their quantum key distribution protocol will find practical application in the near future and will complement existing encrypted communication lines.

“Some basic quantum key distribution networks already exist in Tokyo, Cambridge, Boston and other places,” said Aharonovich. “Instead of using deterministic single photon sources (like ours), they use attenuated lasers that are filtered down to a single photon level.

“They have their own advantages and disadvantages. Quantum key distribution with true single photon sources can be first implemented within metropolitan areas, for instance between government sites within a capital city.”

Aharonovich says they plan to continue improving their technology to make its practical application even more convenient. For example, the photons they use to transmit information have a wavelength of about 645 nanometers, which means they exist in the visible spectrum, while in real-world conditions it may be more convenient to transmit information using significantly longer wavelengths, such as in the infrared range.

“This is important to match [the quantum key distribution to] the existing commercial communication infrastructure,” said Aharonovich.

24.Cybercriminals can break voice authentication with 99% success rate

https://www.helpnetsecurity.com/2023/07/06/voice-authentication-insecurity/

Computer scientists at the University of Waterloo have discovered a method of attack that can successfully bypass voice authentication security systems with up to a 99% success rate after only six tries.

Experts expose flaws in voiceprint technology

Voice authentication – which allows companies to verify the identity of their clients via a supposedly unique “voiceprint” – has increasingly been used in remote banking, call centers and other security-critical scenarios.

“When enrolling in voice authentication, you are asked to repeat a certain phrase in your own voice. The system then extracts a unique vocal signature (voiceprint) from this provided phrase and stores it on a server,” said Andre Kassis, a Computer Security and Privacy PhD candidate and the lead author of a study detailing the research.

“For future authentication attempts, you are asked to repeat a different phrase and the features extracted from it are compared to the voiceprint you have saved in the system to determine whether access

should be granted."

After the concept of voiceprints was introduced, malicious actors quickly realized they could use machine learning-enabled "deepfake" software to generate convincing copies of a victim's voice using as little as five minutes of recorded audio.

In response, developers introduced "spoofing countermeasures" – checks that could examine a speech sample and determine whether it was created by a human or a machine.

Voice authentication insecurity

The Waterloo researchers have developed a method that evades spoofing countermeasures and can fool most voice authentication systems within six attempts. They identified the markers in deepfake audio that betray it is computer-generated, and wrote a program that removes these markers, making it indistinguishable from authentic audio.

In a recent test against Amazon Connect's voice authentication system, they achieved a 10% success rate in one four-second attack, with this rate rising to over 40% in less than thirty seconds. With some of the less sophisticated voice authentication systems they targeted, they achieved a 99% success rate after six attempts.

Kassis contends that while voice authentication is obviously better than no additional security, the existing spoofing countermeasures are critically flawed.

"The only way to create a secure system is to think like an attacker. If you don't, then you're just waiting to be attacked," Kassis said.

Kassis' supervisor, computer science professor Urs Hengartner added, "By demonstrating the insecurity of voice authentication, we hope that companies relying on voice authentication as their only authentication factor will consider deploying additional or stronger authentication measures."

25.Vodafone is preparing for quantum attacks on smartphones

by Faustine Ngila
https://qz.com/quantum-computing-vodafone-security-vpn-smartphones-1850609989

British telecommunications company Vodafone is anticipating a future in which the power of quantum technology will override existing online security controls and render most smartphone networks vulnerable to cyber attacks.

In what it believes is a proactive move, the company has announced that it is teaming up with SandboxAQ, a US startup formerly owned by Alphabet went independent last year, to conduct a proof-of-concept test for a quantum-safe Virtual Private Network (VPN) to secure millions of workers who use their smartphones for business purposes.

SandboxAQ raised $500 million to prepare internet users for a future where cyber attackers deploy quantum computing to hack into the most cyber-tight systems through smartphone networks. Former Google CEO Eric Schmidt is the startup's chairman.

Vodafone wants to protect its customers against cyber attack

In a July 5 blog post, Emma Smith, Vodafone's cyber security director, said that while quantum computing can help in solving some of the world's ultra-complex problems, it could be used by bad actors to crack today's cryptography. "This is why we are playing an active role in the transition to a quantum safe world**,**" she said. Smith said the company's partnership with SandboxAQ will boost its efforts in "exploring and trialing new algorithms to provide protection for our customers against possible quantum-empowered attackers in the future." Vodafone's customer base was over 300 million last year, largely in Africa and Europe.

The two firms will use cryptography algorithms from the US National Institute of Standards and Technology (NIST), which is part of the Department of Commerce, to guard against potential risks from quantum computing, key among them being Store Now, Decrypt Later (SNDL) attacks. Luke Ibbetson, Vodafone's head of research and development said in the blogpost that this type of cyber attack "involves adversaries stealing encrypted data now so they can decrypt it in the future with a quantum computer. Although cryptographically relevant quantum computers may remain some years off, the threat posed by quantum-empowered attackers i s already here today."

In the post, Vodafone says its engineers have been conducting a series of experiments to test several quantum vulnerability scenarios for smartphones because "threat actors may already be harvesting data in anticipation of the quantum computing revolution."

The experiments, Ibbetson explains, involved the assessment of both synthetic traffic data and real data sessions made by internal volunteers from several countries in which the company operates. "We tested the impact of post-quantum cryptography (PQC) on activities many of us do every day," Ibbetson says in the post. These included web browsing, social media, chat applications, video and audio streaming, and mobile gaming "using PQC-enabled mobile handsets, helping to test network performance and assess the user experience."

Governments around the world should prepare for the quantum revolution

Vodafone is a member of the Groupe Speciale Mobile (GSM) Association's newly established Post-Quantum Telco Network (PQTN) task force, which published a white paper in February outlining how governments and mobile network operators should prepare for quantum threats.

The processors in quantum computers run on qubits (subatomic particles such as electrons or photons) rather than the bits (zeros and ones) that power regular PCs. They could one day carry out certain calculations millions of times faster than today's fastest super computers. While Google recently claimed to have assembled a powerful quantum computer, the technology remains years away from breaking complex encryption codes. Encryption involves encoding data in such a way that it can only be decoded by those with access. But with Microsoft announcing in a June 21 blogpost that it plans to launch a powerful quantum supercomputer in the next 10 years, the moment in which quantum technology will land in our smartphones is not far off in the horizon.

The US government already considers quantum computing a critical element of national security, and this could have informed Vodafone's decision to work with a US startup in its security agenda.

On July 5, 2022, the US Commerce Department selected new cryptography standards that could better withstand the threat posed by quantum computers. This was after the US Cybersecurity and Infrastructure Security Agency (CISA) announced the establishment of a Post-Quantum Cryptography (PQC) Initiative three days earlier to unify and drive its efforts to address threats posed by quantum computing.

26.Why cyber pros are nervous about quantum computing Q-Day

by Jonathan Reed
https://securityintelligence.com/news/cyber-pros-nervous-quantum-computing-q-day/

What was once science fiction is quickly becoming science fact. In the past, many wondered if large quantum computers could ever be built. Now scientists believe the post-quantum era to be inevitable.

Recently, IBM unveiled its 433-qubit Osprey quantum computer. This version is more than twice the size of the preceding 2021 Eagle quantum processor. The goal is to scale quantum computing to over 4,000 qubits by 2025.

Does this matter from a security perspective? It does if you ask the Department of Homeland Security about post-quantum cryptography. A quantum computer capable of breaking a public key will need an estimated 6,000 stable qubits, which could occur within a decade. So why are security professionals worried about it now?

Looking ahead to Q-Day

According to a new Deloitte survey, just over half (50.2%) of responding security professionals say that quantum computing risks must be addressed now. These cyber pros believe their organizations are at risk for "harvest now, decrypt later" (HNDL) attacks. HNDL means that intruders extract encrypted data now and save it. Later, when quantum computers are powerful enough, they can break existing cryptographic algorithms and access the data.

This future event has been named Q-Day. Experts believe this phenomenon could occur in the next five to ten years. Without the development of quantum-secure encryption, Q-Day could render nearly all digital information vulnerable to threat actors. When Q-Day arrives, it could impact critical everyday security, including public key infrastructure, HTTP/TLS, network security, payment security, Internet of Things security and blockchain.

Varying levels of worry

Some security teams are already busy at work addressing the quantum threat. Nearly half of respondents (45%) in the Deloitte report expect their organization to complete a post-quantum encryption vulnerability assessment within the next 12 months. An additional 16.2% predict the process will occur within the next two to five years.

Meanwhile, other security pros don't seem to react at all to the threat. Nearly 28% believe their organization's quantum computing security risk response will happen only due to regulatory pressure or demand from company leadership. Other study participants (11.7%) admitted only a cyber incident, such as a sensitive data breach, would cause them to react. Finally, 6.8% of respondents stated that client or shareholder demand would drive change in this area.

Given the potential catastrophe from quantum-based attacks, one wonders why some security pros aren't more worried. What does this say about their current security readiness? Could rising successful attack rates reflect this "wait until we get breached" attitude? Or are security pros swamped with so much work that Q-Day is the last thing on their minds right now?

NIST prepares for Q-Day

Recently, the National Institute of Standards and Technology (NIST) selected the first-ever group of encryption tools that could potentially withstand the attack of a quantum computer. The four winning encryption algorithms will later be incorporated into NIST's post-quantum cryptographic (PQC) standard, which should be finalized in about two years.

According to NIST, the "goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks."

NIST emphasizes the urgency by reminding us that it took almost two decades to deploy our modern public key cryptography infrastructure. So if the post-quantum era will start within ten years, we have our work cut out for us.

Cloudflare has already deployed the Kyber encryption algorithm for its post-quantum library of cryptographic primitives, known as CIRCL (Cloudflare interoperable, reusable cryptographic library). Since 2020, Amazon has supported Kyber as one of its post-quantum key exchange algorithms for TLS 1.2, the encryption protocol behind HTTPS websites. IBM also used Kyber for its first quantum-resistant tape drive.

"NIST constantly looks to the future to anticipate the needs of U.S. industry and society as a whole, and when they are built, quantum computers powerful enough to break present-day encryption will pose a serious threat to our information systems," said Laurie E. Locascio, Undersecretary of Commerce for Standards and Technology and NIST director. "Our post-quantum cryptography program has leveraged the top minds in cryptography — worldwide — to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information."

How to prepare for Q-Day

While NIST has selected four potentially quantum-resistant encryption algorithms, another four may be added soon. Organizations need to be ready to implement these cryptographic algorithms without disrupting infrastructure. Also, they need to be able to switch from one algorithm to another to stay secure against different types of quantum attacks.

During a recent (ISC)² secure webinar, Duncan Jones, head of cybersecurity at Quantinuum, gave some advice about preparing for the coming post-quantum era. The overall strategy includes the following steps:

(I) Gain a clear understanding of your assets and current use of cryptography.
(II) Identify the most significant risks, such as mission-critical and sensitive data, in light of the HNDL risk.
(III) Conduct a collateral risk assessment; ask vendors about their quantum-safe roadmap.
(IV) Create a prioritized migration plan.
(V) Test and experiment sooner, not later.

The post-quantum future

What was once science fiction is now likely to happen within a decade. Quantum computing will usher in an entirely new era of cyber challenges. Today, while security pros combat phishing, ransomware, distributed denial-of-service and social engineering attacks, a more dangerous threat gathers steam. It would be prudent to start Q-Day readiness plans now.

27.Quantum Cryptography Challenges and Opportunities for Federal Agencies

by Nathan Eddy
https://fedtechmagazine.com/quantum-cryptography-challenges-opportunities-perfcon

In 2016, the National Institute of Standards and Technology asked experts to develop quantum-resistant public-key cryptographic algorithms algorithms that could be standardized for use in protecting sensitive government information. Five years later, in July 2022, the top four candidates were announced.

Less than a month after that, however, researchers using only a single-core classical computer were able to break one of NIST's runners-up (named, ironically, SIKE) in just about an hour.

Transitioning critical infrastructure toward federally approved post-quantum cryptography (PQC) standards remains a challenge for private and public sectors, but proper implementation of these standards will protect data, the government and the country itself from adversaries in a way not seen before, NIST experts say.

"NIST constantly looks to the future to anticipate the needs of U.S. industry and society as a whole, and when they are built, quantum computers powerful enough to break present-day encryption will pose a serious threat to our information systems," said NIST Director Laurie E. Locascio in a news release.

The federal government is in the process of assessing the potential impact of quantum computing on its operations and infrastructure to prepare for the future of post-quantum cryptography.

What Is Quantum Cryptography?

Quantum cryptography leverages the principles of quantum mechanics to create secure communication channels. It encodes information into a quantum system created from collections of tiny particles such as protons and transmits them to create a key that can decrypt the data.

Natasha Eastman, chief of operations for threat hunting at the Cybersecurity Infrastructure and Security Agency (CISA), explains that quantum computers themselves are inherently different than classical computers.

"Classical computers run a series of one and zeros, while quantum computers run zeros and ones all at the same time and ultimately allow the creation of algorithms that process information much, much faster than classical computers," she says.

Instead of occurring one at a time, calculations can occur at an astronomically higher speed. Quantum computing also provides the means for more complex encryption that is more difficult to decode, because the possible numbers of encryption combinations is nearly infinite.

The mathematical strength of asymmetric cryptography — another name for public-key cryptography, which uses one public key and one private key to encrypt and decrypt data — lies in two areas, Eastman says:

- There is no one method to solve discrete logarithmic problems

- There is not one method to factoring large integers to break them down into smaller, prime numbers

Both calculations are necessary to develop an encryption key. But as methods are developed to better process data inherent to quantum computing, some could threaten the current implementations of asymmetric cryptography, as well as some implementations of symmetric cryptography (based on single keys to decode information).

“That threat to the security of modern cryptographic algorithms is really where we’re concerned, how that will change the nature of how we protect information,” Eastman notes. “Obviously, quantum computing also can be a benefit to how we protect information in cybersecurity.”

CISA and other security agencies and experts are concerned about the next 10 to 15 years in the quantum transition, when they expect the development of a cryptographically relevant quantum computer that could threaten even the most modern cryptographic algorithms protected from classic computers.

How Is Post-Quantum Cryptography Different?

Post-quantum cryptography does not require quantum technologies; instead, it is designed to protect against them.

Quantum cryptography harnesses the properties of quantum mechanics to secure and transmit data in a way that cannot be hacked. Quantum cryptography uses photons — individual particles of light — to transmit data over fiber-optic wires.

Photons are an integral part of providing a secure method for key encryption: quantum key distribution (QKD), which uses a shared private key between two connected parties. Data and the key are both transmitted via photons over optical fiber cable.

The key exchange is based on the Heisenberg uncertainty principle, which states that a person can’t calculate both the position and speed of a particle accurately; the more accurate you get on one, the less accurate you get on the other.

In the case of QKD, photons are generated randomly in one of two polarized quantum states, making the measurement of the quantum property of a photon impossible without altering the quantum information itself.

In such a path, the two endpoints of communication can verify the shared private key; it is safe to use if the photons are unchanged. If a malicious actor intercepts or accesses the message to learn the key, the quantum properties of the photons are altered.

If even a single photon change is detected, both legitimate parties understand the message has been compromised and is not safe to be trusted.

How Does Post-Quantum Cryptography Work?

Post-quantum cryptography, also known as quantum-resistant cryptography, goes a step further than quantum cryptography, says Priti Patel, a security consultant at Coalfire.

“The goal is to develop cryptographic systems that are secure against both quantum and classical computers and that have the ability to interoperate with existing communications protocols and networks,” she says.

NIST's post-quantum cryptographic standard is expected to be finalized in the next year, but the agency already has resources available, including a white paper titled "Getting Ready for Post-Quantum Cryptography" and a draft version of NIST SP 1800-38A, "Migration to Post-Quantum Cryptography."

"It is imperative to perform risk assessments specific to each agency, department and critical infrastructure operation," says Jeffrey Wells, partner at Sigma7. "These assessments will involve meticulously evaluating vulnerabilities, potential attacks and risks associated with quantum computing."

By conducting such assessments, organizations can proactively identify areas of concern and develop targeted mitigation strategies. These should include deploying quantum-resistant algorithms and encryption methods and diversifying cryptographic systems.

"Taking these proactive measures will help safeguard sensitive data, protect communication channels and ensure the continued resilience of operations in the face of potential quantum threats," Wells says.

Should Feds Consider Using Quantum Cryptography?

The next step for federal agencies and the entire government is to figure out the challenges that come with post-quantum cryptography, Patel says.

For instance, replacing an algorithm normally requires changing or replacing cryptographic libraries; implementing various new tools and hardware, dependent operating systems and code; and adhering to certain protocols and procedures, among other issues.

"An important step to begin migrating from the current set of public-key algorithms to post-quantum algorithms includes identifying where and for what purpose public-key algorithms are being used," Patel says.

The federal government is working to begin implementing post-quantum cryptography, she says. "Is it still a long journey ahead? Yes. However, these publications, roadmaps and guidance, if harnessed properly, will create a stronger future as well as stronger government alignment and implementation of these practices into our daily processes."

A November 2022 memo from the Office of Management and Budget, "Migrating to Post-Quantum Cryptography," states that building an inventory is a critical first step. This inventory will include systems that agencies use or that are operated on behalf of that agency, including high-impact information systems and high-value assets.

Next steps include preparing funding assessments that estimate how much migration to post-quantum cryptography could cost. The White House wants federal agencies to transfer to PQC systems by 2035.

"It's important we start on this migration to post-quantum cryptography now since this is a lengthy process with many inherent challenges," Patel says. "This must be treated as a priority."

28.Protecting Connected Devices with Quantum-Generated Cryptographic Keys

by Berenice Baker
https://www.iotworldtoday.com/security/protecting-connected-devices-with-quantum-generated-cryp-

tographic-keys

Quantum computing company Quantinuum last week Quantinuum released Quantum Origin Onboard, a cryptographic innovation that provides quantum computing protection for connected devices.

In this Q&A, Quantinuum head of cybersecurity Duncan Jones explains the challenges of protecting connected devices, how a quantum computer helps generate cryptographic keys that are as unpredictable as possible, and the importance of protecting essential assets like critical infrastructure and banking systems.

Enter Quantum: What is Quantum Origin Onboard?

Duncan Jones: Quantum Origin is something we launched a couple of years ago. It helps customers to generate strong cryptographic keys using quantum computing. We plug into their existing cyber infrastructure and we generate cryptographic keys for them that we can mathematically prove are unpredictable, which is the main ingredient that you want to have in a cryptographic key.

Quantum Origin Onboard is a new variant of this product that you can plug into your infrastructure. Some customers said we want to put this everywhere in our infrastructure, and some of our infrastructure is disconnected, in an air gap system. Quantum Origin Onboard is a software library that you can put into a device or a system, and it helps that system generate stronger keys.

What are the cybersecurity challenges presented by IoT infrastructure?

Typically, IoT devices are not renowned for security; it is an area of usually higher cyber risk for a company when they deploy IoT devices. One of the reasons why we're excited to start putting Quantum Origin Onboard into IoT devices is because they do need strengthening against cyber risks; they're out there, on the frontline.

They're often deployed for decades, so if you make a mistake from a security perspective, it can be very costly to fix. Industrial IoT systems in critical national infrastructure are a good fit for the Quantum Origin Onboard. It is also suited to air-gapped corporate IT systems where cloud service isn't appropriate.

Quantum Origin Onboard uses a “quantum seed”, what is that?

We execute a three-qubit circuit on our H-Series computers, and we do that millions and millions of times to build up a collection of challenges to the quantum computer and responses from the quantum computer.

We pass that data through a Bell test, which we use to quantify the amount of unpredictable behavior we've just witnessed. What comes out of that process is a relatively small piece of data of a few 100 kilobytes which is of an unknown amount of randomness.

At this stage, we know that it's 84% perfect and once we know what it is, we can distill it into what we call the quantum seed, which is a piece of data that is as highly unpredictable as possible. We have a very strong mathematical guarantee of how predictable that is.

Are post-quantum cyberattacks one of the threats you’re strengthening systems against?

A lot of the organisations we're working with are thinking about the threat of quantum and they want to adjust both the way that they generate the keys and the type of keys they generate to make sure that both are resilient.

We have not invented a new type of encryption; we work with whatever the customer chooses to use. Many of our customers are still using today's algorithms like RSA or elliptic curve cryptography. But some are starting to look at quantum-safe algorithms as well. We support both, but the way that we generate our keys and that guarantee of unpredictability will hold universally and that will still be true in 20 years, regardless of the quantum computing power of your adversary.

What companies would use Quantum Origin Onboard?

Anybody who is generating cryptographic keys, which these days is every industry. Our focus areas have been initially around financial services, utilities and critical national infrastructure clients – the places where cybersecurity is often of the highest importance because these companies have to retain the trust of their customers.

In banking, you must trust that the bank is going to be able to protect your money. But critical infrastructure areas it's also a life safety question, as well as the people hacking the system. People can die, so that's been our initial focus. But ultimately, this technology is broadly applicable, and we anticipate this becoming the de facto approach to generating keys over time.