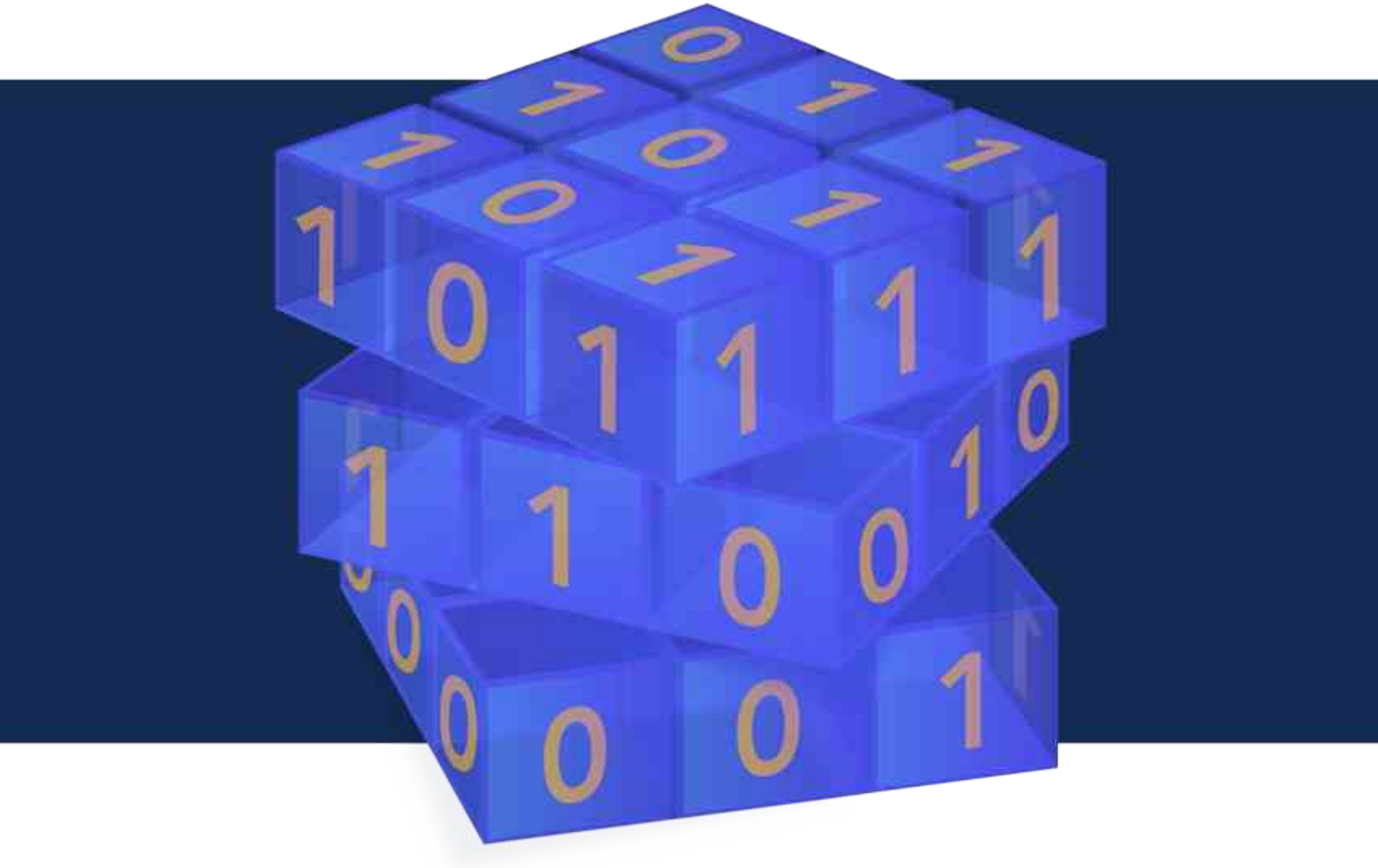
Crypto News

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

March 01, 2022



Editorial 5

SEATTLE, WA – March, 1st, 2022. The warmth of spring is only a few weeks away. While we all wait for the weather to get better, I'll be snuggling up with this month's issue of Crypto News. Let's get started! Have you been struggling with programming quantum algorithms? Are you getting too many errors and spending too much time debugging? Well, there's hope with MIT's new quantum programming language, Twist. It helps programmers know when qubits are entangled and when they are not. Though more work is needed to show which qubits are entangled specifically, Twist is a useful baseline to build upon for future programming languages. Future languages can work at a more granular level to show which qubits specifically are entangled, their phase, and even if they are in superposition or not. Take some time to scroll down to article #12 for more information. 5

If you work in the Aerospace or Defense industries then article #19 is for you. There is a mysterious group of hackers dubbed TA2541 active since 2017 who have distributed malware via phishing emails to hundreds of organizations across North America, Europe, and the Middle East. They distribute different types of malware, gain remote access to network assets, and steal data. The disturbing part is that they are still at large and governments are no closer to identifying the culprits. Make sure to read the article for more details that may help you train your organization's personnel on these attacks so they do not fall prey to them. 5

Last but not least, if you work in any cybersecurity role, then take the time to read article #29. Are you willing to start preparing now for the impending and astronomically impactful changes that the widespread use of quantum computing will bring? With all new innovations, we are made well aware of the positives of the innovation as it is being developed and released on a larger scale. An interesting aspect of quantum computing as a new innovative technology is that we are also well aware of the drawbacks and threats this technology poses. This provides us with the unique opportunity to not only prepare for, but thrive in a post-quantum world by addressing the well known drawbacks and threats now. Take a look at the "Preparing for a post-quantum world" section of the article for steps you and your organization can start taking now to prepare. Don't forget to take the time to peruse the other articles in this newsletter and get up to speed on all things cybersecurity and quantum computing. Happy reading! 5

Crypto News is authored by Dhananjoy Dey with this editorial provided by Mehak Kalsi. Both are active members of the Cloud Security Alliance (CSA) Quantum-Safe Security Working Group (QSS WG). The guiding principle of the QSS WG is to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting their networks and their data. 5

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. 5

1.What Does the Breaking of Rainbow Mean for Cybersecurity? 6

2.INDIA JOINS RACE to WEAPONIZE QUANTUM TECH in FUTURE MILITARY CONFLICTS 7

3.Cryptographer – Job Description and How to Become 9

4.DRDO successfully tests Quantum Key Distribution tech between 2 cities 12

5.The Engine to Run the Post-Quantum Future is Here 13

6.The threat of quantum computing to security infrastructure 13

7.JPMorgan Chase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application 15

8.Israel’s Microsoft of quantum computing makes its move 17

9.How quantum computing could transform the world 18

10.Biden's cybersecurity order opens our post-quantum era 20

11.Cryptographic Agility: Exploring Proxy Approaches 22

12.Meet Twist: MIT’s Quantum Programming Language 26

13.China releases new quantum computing software 28

14.JPMorgan Chase readies for post-quantum security world 28

15.Infineon IC addresses post-quantum security 30

16.Quantum Cryptanalysis: Hype and Reality 31

17.Quantum errors made more tolerable 37

18.Rigetti Computing Announces Commercial Availability of 80-Qubit Aspen-M System and Results of CLOPS Speed Tests 39

19.Warning over mysterious hackers that have been targeting aerospace and defence industries for years 40

20.Quantum errors made more tolerable 42

21.Quantum leap: Has next-gen computing moved from hype to hope? 43

22.Two-dimensional material could store quantum information at room temperature 45

23.An Introduction to Post-Quantum Public Key Cryptography 46

24.Tips to mitigate public-key cryptography risk in a quantum computing world 51

25.Duke University, IonQ’s New Quantum Computing Gate Could Lead to More Efficient Quantum Algorithms 53

26.Race Not Over Between Classical and Quantum Computers 54

27.Equinix and SK Telecom to provide quantum cryptography between data centers 55

28.Germany Expands its Quantum Computing Roadmap with QuaST 57

29.Re-think security today for a post-quantum world tomorrow 57

30.Quantum Computing Lab Opens in London, Aims to Build World’s Largest Quantum Computer 59

31.The race to save the Internet from quantum hackers 61

32.NTT Scientists Advance Post-Quantum Cryptography at FOCS Symposium 63

33.6 reasons we need to start thinking about quantum computing now 64

34.New Super-Conducting Technology Takes Data Beyond Ones and Zeroes 66

35.Quantum Computing: Researchers Achieve 100 Million Quantum Operations 68

36.Jian-Wei Pan: ‘The next quantum breakthrough will happen in five years’ 69

37.Observation of quantum transport at room temperature in a 2.8-nanometer CNT transistor 71

38.Scientists estimate that quantum computers may become powerful enough to crack the Bitcoin encryption in a decade 72

39.Quantum Computing Guidelines Issued by World Economic Forum 73

40.Meet the NSA spies shaping the future 75

41.The power of chaos: A robust and low-cost cryptosystem for the post-quantum era 79

42.Efficient Quantum Programming Using Ease Gates on A Trapped-Ion Quantum Computer 80

Editorial

SEATTLE, WA - March, 1st, 2022. The warmth of spring is only a few weeks away. While we all wait for the weather to get better, I'll be snuggling up with this month's issue of Crypto News. Let's get started! Have you been struggling with programming quantum algorithms? Are you getting too many errors and spending too much time debugging? Well, there's hope with MIT's new quantum programming language, Twist. It helps programmers know when qubits are entangled and when they are not. Though more work is needed to show which qubits are entangled specifically, Twist is a useful baseline to build upon for future programming languages. Future languages can work at a more granular level to show which qubits specifically are entangled, their phase, and even if they are in superposition or not. Take some time to scroll down to article #12 for more information.

If you work in the Aerospace or Defense industries then article #19 is for you. There is a mysterious group of hackers dubbed TA2541 active since 2017 who have distributed malware via phishing emails to hundreds of organizations across North America, Europe, and the Middle East. They distribute different types of malware, gain remote access to network assets, and steal data. The disturbing part is that they are still at large and governments are no closer to identifying the culprits. Make sure to read the article for more details that may help you train your organization's personnel on these attacks so they do not fall prey to them.

Last but not least, if you work in any cybersecurity role, then take the time to read article #29. Are you willing to start preparing now for the impending and astronomically impactful changes that the widespread use of quantum computing will bring? With all new innovations, we are made well aware of the positives of the innovation as it is being developed and released on a larger scale. An interesting aspect of quantum computing as a new innovative technology is that we are also well aware of the drawbacks and threats this technology poses. This provides us with the unique opportunity to not only prepare for, but thrive in a post-quantum world by addressing the well known drawbacks and threats now. Take a look at the "Preparing for a post-quantum world" section of the article for steps you and your organization can start taking now to prepare. Don't forget to take the time to peruse the other articles in this newsletter and get up to speed on all things cybersecurity and quantum computing. Happy reading!

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

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

1.What Does The Breaking of Rainbow Mean for Cybersecurity?

by Duncan Jones
https://medium.com/cambridge-quantum-computing/what-does-the-breaking-of-rainbow-mean-for-cybersecurity-21b125383cab

A paper was released this week with the provocative title: Breaking Rainbow Takes a Weekend on a Laptop. The author is a cryptographic researcher, and the paper outlines an attack on Rainbow, a finalist of the NIST post-quantum cryptography (PQC) process. If the contents of the paper are correct, the implication is that Rainbow is no longer a good candidate for adoption.

This new attack provides a timely reminder that many aspects of cryptography rely on computational complexity arguments. Put simply, the security of an algorithm is derived from the fact that nobody has figured out a way to break it in a reasonable amount of time. If it takes three million years on a supercomputer to break a cryptographic algorithm, it's probably safe for use today.

Most cryptographic algorithms have parameters that provide different levels of security. For instance, RSA keys can be generated in different sizes, depending on how secure the key needs to be. 512-bit RSA keys were once considered adequate for security, but now we know longer keys are needed to defend against improved attacks and increasing computing power. However, the longer we make the keys, the more impractical an algorithm becomes, so it's important to balance practicality with security.

In the NIST selection process, each PQC algorithm is required to provide parameters that meet three increasing security levels (SL1, SL3 and SL5). In the paper, the author proposes an attack that can break the SL1 parameters, meaning that Rainbow cannot safely be used without increasing key lengths and signature sizes. These changes would make the algorithm far less attractive, since it would be more difficult to integrate it into existing systems. It's plausible further breakthroughs would lead to more efficient attacks that render even these larger keys vulnerable to attack.

It's not a surprise to see a PQC algorithm successfully attacked in this fashion. After all, humans are ingenious and computers are getting more powerful. Rainbow is far from the first algorithm to be found wanting by the selection process. You might argue, correctly, that the purpose of the process is to achieve this type of elimination. However, every time a new attack is discovered, we should reflect on whether we are on the right path, when it comes to securing our cybersecurity systems.

Unlike cybersecurity systems derived from computational complexity, quantum cybersecurity offers a range of tools that rely on the laws of physics. When we use quantum technologies to generate a cryptographic key, for instance, we are relying on quantum mechanics to ensure the key is strong. There is no algorithm that could be broken by smart thinking or a faster computer. It's a fundamentally different approach. No advances in cryptanalysis or computing will result in the ability to predict how the universe behaves at such a basic level.

Computational complexity will continue to play its part, and we will always need classical algorithms to build security systems. However, this paper reminds us that new attacks can appear at any moment if you rely on complexity as your defence. Now that quantum cyber technology is a reality, companies should consider where they can switch from complexity-based thinking to defences built using the fundamental laws of nature.

2.India Joins Race to Weaponize Quantum Tech in Future Military Conflicts

https://idrw.org/india-joins-the-race-to-weaponise-quantum-technology-in-future-military-conflicts/

On February 23, the Defence Research and Development Organisation (DRDO) made an announcement that went a bit under the radar but can have huge ramifications in the future for developing military technologies. The official statement given by the DRDO stated that a joint team of DRDO and IIT-Delhi successfully demonstrated a Quantum Key Distribution (QKD) link for the very first time in the country between the cities of Prayagraj and Vindhyachal in the state of Uttar Pradesh. An interesting thing to note is that these cities are located at a distance of 100 kilometres from each other. This marks the beginning of the Indian military complex utilising an emerging technology like quantum to enhance domestic defensive capabilities.

The Potential Warfare Applications

The second quantum revolution witnessed in the past decade threw open many possibilities of developing credible commercial applications using quantum technology. It also led to the possibility of using quantum technology in the security and military domain. While military applications using quantum tech are still in the process of development, it is imperative to recognise the ability of this kind of technology to gain an upper hand when it comes to the security aspect.

From a communications perspective, there is a high chance of using state-of-the-art quantum computers to subvert encrypted systems and conduct unlawful surveillance. China's quantum satellites have been touted as potential devices that be used to gain unauthorised access to crucial information. Even modern-day security systems seem to be vulnerable to the emergence of such technologies. Hence, there have been efforts to build secure systems using new technologies like quantum to ensure encryption and privacy remain uncompromised. Such new mechanisms include quantum cryptographic systems and quantum key distribution (QKD) systems. The recent announcement of the DRDO also shows that the Indian military is now looking at developing indigenous technology of secure key transfer for bootstrapping military-grade communication security.

There is now the issue of using sensors, based on quantum technology in the detection of both underwater submarines and aerial military vehicles. The increased use of unmanned aerial vehicles (UAVs) in the military domain has also led to quantum sensing playing a major role in optimising drone movements. Precision guidance and geo-positioning remain critical applications that require the use of these quantum-based sensors. Based on the working principle of entangled photons, a pattern is created showcasing the presence or absence of a target object. The advantage of this sensing technology remains high accuracy regardless of the amount of noise in the system.

States Crossing The Quantum Barrier

This begs the question of the potential role played by quantum-based military technology in future wars and conflicts. With leaps made by China in the quantum domain, there is a fear of the Chinese military developing both offensive and neutralising capabilities using this kind of technology. Reports on the development of quantum radar have been heard from China which can have devastating consequences on current stealth technology. A detection system such as quantum radar is capable of not only determining the type of incoming enemy aircraft but also the type of weapons being carried in the vehicle itself.

The development of a quantum submarine detector (made up of extremely sensitive quantum sensors), named SQUIDS (Superconducting Quantum Interference Devices) has been reported by the Chinese National Academy of Science. This technology is capable of detecting underwater submarines from long distances giving a huge advantage in the maritime domain also. If the reports hold true, then we might have to be prepared for the Chinese military gaining an immense advantage with future warfare capabilities.

Considering the current situation in Ukraine, it is also possible that Russia has been investing in developing high-trade military technology. The comments made by President Vladimir Putin and the deputy Prime Minister in charge of the military-industrial complex, Yuri Borisov, have reiterated Russia's commitments to building state-of-the-art weapons systems utilising the 'principles of new areas of physics'. This was meant to highlight the country's advancements and expertise in areas like plasma and quantum physics to make improved weaponry systems. Recent Department of Defence (DOD) reports by the United States government have also indicated how the Russian military has been focusing on electro-warfare capabilities using dedicated quantum technology.

Other quantum powers such as Australia have also been actively trying to make a mark in the field. Researchers and scientists in the country working on developing quantum technologies have been trying to find applications related to the military itself. There have already been deployments of quantum tech in areas like the cryogenic sapphire oscillator, also called the Sapphire Clock, for improving radar efficiency. The advantages offered across terrains and other conditions have made the country's military scientists look at quantum technology as an alternative solution to military-grade GPS currently in use. The 'Army Quantum Technology Roadmap' by the Australian Army explores the potential solutions across sensing, communications, and computing that quantum tech can offer to the military in the long run.

Finally, even the United States government and armed forces have gotten into the sector. The Defence Science Board (DSB) of the US military and an independent board within the Department of Defence (DOD) have made quantum tech research an important area of focus. The DSB, made of the country's top scientific advisors helps give direction to the military on scientific research of new weapons and technology. The 2019 National Defence Authorization Act (NDAA) directs the Secretary of Defence to set up a quantum technology research and development program to work with the private sector and other government groups. The 2020 NDAA also mentions the need for the DOD to develop certain ethical guidelines for using quantum technology in military applications. This shows how the US military and defence department are not actively involved in providing funds for research in the field but also involved in framing standards and best practices of using said technology.

It is clear that the frontiers of quantum technology in the military domain have already been breached with immense capital being poured into the field by multiple states across the globe. While some have actively demonstrated the effects of such technologies, there still exists questions on how they might actually play out when deployed on the ground in actual conflicts. Military quantum technology is here but do we have the necessary tools and competence to regulate its use is the question that still needs to be answered.

3.Cryptographer – Job Description And How to Become

by Wallarm
https://lab.wallarm.com/cryptographer-job-description-and-how-to-become/

Cryptography is perhaps the main instrument for building a secure computerized framework. These professionals assume a major part in building these frameworks. This makes them probably the most generously compensated and profoundly esteemed labourers inside the growing universe of cybersecurity. A profession as a cryptographic expert can be testing and remunerating both mentally and financially. Assuming that you're considering a job as this type of specialist, there's a great deal you should know and much you ought to learn. This guide will assist you with finding more about what a cryptographic expert is, their main roles, and investigate the IT degrees you can seek after to get ready for this intriguing profession.

Who is a Cryptographer?

A cryptographer is a person who composes (or breaks) the encryption code utilized for information security. PC encoded information utilizes astoundingly lengthy, progressive encryption calculations that are unimaginably hard and tedious for individuals to break. Today, online encryption administers the information trade between web hosts and internet browsers and is basic to stable web-based exchanges, secure correspondences, and safe information trades.

Cryptography is a basic component inside the more extensive field of cybersecurity. As the requirement for better web-based security develops, the requirement for these experts will just keep on expanding. Make sure to dive deeper into cryptographic occupations, the cryptography pay, and how to turn into a cryptographer so you can get your future in this intriguing field.

What Does a Cryptographer Do?

As a cryptographer, you'll assist with creating complex security frameworks utilizing codes and calculations to scramble delicate information and safeguard it from programmers, abuse, and cybercrime.

This safeguarded data may include monetary, individual, business, or military information. Cryptographers utilize various private key or mystery key codes to assist with encryption. They can utilize RSA public keys, advanced marks, and other encryption procedures to assist with guaranteeing their work is secure.

Your normal obligations will be numerous and fluctuate contingent upon what kind of association you work for. Most organisations focus on safeguarding information from being blocked, decoded, replicated, adjusted, or erased by unapproved entertainers. In this way, you'll require a strong comprehension of cryptographic security frameworks and their connected calculations. You'll likewise create and apply different measurable and numerical models to help find and impede potential framework dangers.

The everyday obligations of a cryptographer may include:

- Recognizing and eliminating shortcomings in existing cryptography frameworks.
- Testing cryptology speculations according to your association's necessities.
- Improving information security through the execution of safer and encoded arrangements.
- Utilizing public key cryptography with RSA or other code types.
- Using secret key, private key, and public key cryptography to support encryption objectives.
- Creating and dealing with your association's encryption technology, including its code, programming, and outsider item reception.
- Prototyping new security arrangements with cutting edge programming encryption strategies and practices.
- Preparing other staff that handles encryption information and assisting them with creating free from any and all harm frameworks.
- Attempting to decode data and if necessary to track down weaknesses in the system

Skills for a Cryptographer

Cryptographers need information on PC frameworks, organization, and data set engineering. They also need knowledge of information designs and algorithms, including advanced science abilities. Cryptographers should comprehend different types of numerical hypotheses and apply ideas and procedures to mathematics calculations. Cryptograph experts likewise know numerous programming dialects and basic programming languages such as Python, Java, and C++.

Through understanding data security programming and equipment, cryptographers have knowledge of security arrangements. Experience in data innovation support improves these abilities. Cryptographers also have insight with working frameworks, including Microsoft Windows and UNIX. They know how to use WAF to bolster API security.

Cryptographers use encryption calculations in view of symmetric and unbalanced key-block figures. Normal calculations incorporate Triple Data Encryption Algorithm (Triple DES) and Rivest-Shamir-Adelman (RAS). Triple DES safeguards against security attacks by applying a symmetric-key square code multiple times to every informational collection. RAS was one of the principal generally utilized public-key cryptosystems for information transmission.

Through examination and decisive reasoning, cryptographers foster calculations and codes to get delicate data. They make security arrangements by distinguishing, amending, and alleviating existing and future dangers. Cryptographers likewise decipher scrambled data, interpreting it to get close enough to security conventions and secure substance.

Cryptographers need solid verbal and nonverbal communication abilities. As people entrusted with information encryption and decoding, they frequently fill in as a component of a group. Cryptographers hand-off their discoveries to partners, giving itemized clarifications of their practices and cycles. They may likewise disclose specialized ideas to non-specialized experts, making confounded ideas and thoughts open to general crowds.

How to Become a Cryptographer?

To turn into a cryptographer you should initially procure a four year certification in software engineering, information technology, cybersecurity, or math. These disciplines show the specialized, quantitative, and rational abilities required for making and breaking complex modern-day codes. Coursework creates essential knowledge and skills in arithmetic, PC and data innovation frameworks, and programming languages. Aspiring cryptographers need solid numerical abilities. They might finish a twofold major, concentrating on mathematics along with a PC related discipline. A mathematics major underscores the information structures, theoretical variable based math, and calculations fundamental for a vocation in cryptology.

Most cryptography occupations expect no less than five years of involvement with PC and data information security. Entry-level roles, such as programming developers, data security investigators, or PC framework examiners gain experience with data innovation security equipment and programming. A mid-level job as a data innovation specialist of organization and PC framework director can likewise give future cryptographers an understanding into data innovation plans, organization, and authority.

Assuming you're thinking about working for the military or Department of Defense, you may likewise need to concentrate on semantics or an unknown dialect since your job might relate to unfamiliar correspondence signals. Furthermore, postgraduate education, for example, a Master of Science in Cybersecurity and Information Assurance helps to give you an edge in getting more lucrative, more aggressive positions. Furthermore, a large number of these highly favored jobs expect something like five years of experience too.

Regardless of any job you pick, cryptologists should regularly update their ability and pertinence through consistent learning. Systems and technologies are continually evolving. So to keep up, you can join a proficient association like the International Association for Cryptologic Research or acquire some work explicit confirmation like the ECES.

How Much Is a Cryptographer Salary?

With an expected 12% development in work somewhere in the range of 2018 and 2028, PC and data innovation occupations are anticipated to have solid additions. As indicated by PayScale, cryptographers procure normal compensations simply more than $125,179.

A Cryptographer job description is the same, regardless of whether they work for the government, innovation, or monetary sector. The Department of Defense and the National Security Agency utilize cryptographic experts to safeguard military, public safety, and online protection frameworks and information

New York	Los Angeles	Chicago	Houston	Phoenix
$136,981/yr	$140,147/yr	$134,326/yr	$129,367/yr	$121,003/yr

Data innovation organizations like Microsoft, Amazon, and Apple need cryptographers to safeguard their information close to their clients and purchasers. Banks, venture companies, and bookkeeping organizations likewise depend on cryptographers to get private monetary data.

4.DRDO Successfully Tests Quantum Key Distribution Tech Between 2 Cities

by IANS
https://www.business-standard.com/article/current-affairs/drdo-successfully-tests-quantum-key-distribution-tech-between-2-cities-122022301259_1.html#:~:text=A%20joint%20team%20of%20scientists,of%20more%20than%20100%20km

A joint team of scientists from Defence Research and Development Organisation (DRDO) and the Indian Institute of Technology (IIT) Delhi, for the first time in the country successfully demonstrated Quantum Key Distribution link between Prayagraj and Vindhyachal in Uttar Pradesh, a distance of more than 100 km.

Quantum key distribution is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.

This technological breakthrough was achieved over a commercial grade optical fibre already available in field. With this success, the country has demonstrated indigenous technology of secure key transfer for bootstrapping military grade communication security key hierarchy, the DRDO said.

The performance parameters have been measured and have been found to be repetitively within the reported international standards at sifted key rates of up to 10 KHz. This technology will enable security agencies to plan a suitable quantum communication network with indigenous technology backbone.

The Secretary Department of Defence R&D and Chairman DRDO Dr G Satheesh Reddy congratulated the scientists and faculty of DRDO and IIT Delhi for the demonstration of this technology. In his message to the involved scientific fraternity, he mentioned this as one of the shining examples of synergetic research between DRDO and Indian Institute of Technology, Delhi.

Director of IIT Delhi, Professor Rangan Banerjee also congratulated the faculty and scientists of

DRDO associated with this development for their dedicated efforts to enhance country's technological capability.

5.The Engine to Run The Post-Quantum Future Is Here

by PR.com
https://www.benzinga.com/pressreleases/22/02/r25770997/the-engine-to-run-the-post-quantum-future-is-here

The QRL Foundation, supporting the Quantum Resistant Ledger (QRL) post-quantum secure blockchain, and in partnership with Geometry Labs, are pleased to announce "lattice-algebra," an elegant, high-performance, cryptographic library on GitHub for use in blockchain systems integrating post-quantum security. This includes projects moving to Proof-of-Stake, like QRL and Ethereum, allowing for the clean implementation of cryptographic schemes such as zero-knowledge proofs and signature aggregation.

The "lattice-algebra" library will be used to prototype a variety of new features for the Quantum Resistant Ledger (QRL) protocol, such as lattice-based Proof-of-Stake signatures, trustless cross-chain atomic swaps (QRL↔BTC, QRL↔ETH, etc), and "lightning network" style payment channels.

Without the 'lattice-algebra' module, lattice cryptography developers would have to divert time and resources towards rolling their own implementation of the underlying math, which is an anti-pattern that leads to duplicated, unoptimised, and difficult-to-maintain code. Unifying everything allows developers to write clean code that securely implements post-quantum cryptography for protocols and applications.

One key feature enabled by unification is being able to split the audit surface, where the "lattice-algebra" library could undergo a preemptive audit, giving downstream cryptographic applications a head start on their own audits. This is done by allowing developers and researchers to work with a few high level objects (e.g. polynomials, polynomial vectors) that contain built-in methods to abstractly handle the ways that they interact with each other. Schemes based on other hardness assumptions (such as the Ring Learning With Errors assumption) that take place over the same ring can be securely implemented as well. More details are covered in QRL's lattice-algebra blog.

6.The Threat of Quantum Computing to Security Infrastructure

by Henry Kressel
https://asiatimes.com/2022/02/the-threat-of-quantum-computing-to-security-infrastructure/

Quantum computers as conceived are radically different from the familiar digital machines in use today. They operate by leveraging unique phenomena in quantum physics of materials (based on the behavior of sub-atomic particles) to enable computations to be performed that can enable the rapid solution of certain problems in minutes that could take years with conventional high-performance computers.

They don't exist yet and formidable engineering problems have to be overcome for their potential to be realized. In particular, achieving reliable computation is known to be a major challenge. But enough research progress has been made to suggest that such computers could be built eventually.

Major resources are being devoted to this task in the US, China and elsewhere, with researchers at Google in the US among the leaders striving to solve the formidable engineering problems.

What is unusual about this endeavor to achieve new computing capabilities is the public-policy interest. The ongoing research on quantum computing is generating enormous government-agency interest at a time when its practical value has not been demonstrated.

This level of interest is unusual at such an early technology stage and is unprecedented in digital history. But the reason is clear. If successful, such computers will threaten to render obsolete strategically critical cryptographic software that protects much of the most sensitive information in the world.

Hence the interest in developing cryptographic software that will not be able to be broken by quantum computers as currently conceived. In fact, in 2015, the US National Security Agency called for a transition to new algorithms that would be safe from quantum computers.

I can't think of an emerging electronic technology that has generated as much dread and anticipation, because different and more powerful computers not only promise to change cryptograph software technology - a negative - but on the positive side allow simulation of complex physical and chemical systems too challenging for current supercomputers.

Such simulation opens the door to new drugs and chemical products. But not surprisingly, it is the challenge to existing data security that prompts the most immediate concerns and will trigger the most investment in countermeasure solutions both in the private and public sector.

Here are some examples of government activity to develop protective software resources.

In Canada, a report titled "Canadian National Quantum - Readiness" was issued on July 7, 2021, to describe best practices and guidelines for developing new software to overcome the quantum-computing threat.

The report states:"The encryption technologies that are securing Canada's financial systems today will one day become obsolete. If we do nothing, the financial data that underpins Canada's economy will inevitably become more vulnerable to cyber criminals."

In the US, as noted above, the National Security Agency took an early lead in identifying the perceived threat.

On January 19, 2022, an action from the US president came public. The White House issued a "Memorandum on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems."

The document shows the urgency needed to address perceived major threats. It outlines major actions to avoid security lapses that would be created by quantum computers targeting critical secret data and related infrastructure. It also identifies the management responsibilities in the various agencies to implement these measure within a matter of months.

This perceived threat to existing cybersecurity will generate a great deal of private industry and bring well-funded new companies into the business of transition to new security solutions.

It is clear that well-informed experts believe that powerful new quantum computers will emerge and that the risks are so great of their ability to overcome existing security barriers that an all-out effort is needed to build safeguards now.

7.JPMorgan Chase, Toshiba And Ciena Build The First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application

by Jennifer Lavoie
https://www.jpmorganchase.com/news-stories/jpmc-toshiba-ciena-build-first-quantum-key-distribution-network

In groundbreaking research, JPMorgan Chase, Toshiba and Ciena have demonstrated the full viability of a first-of-its-kind Quantum Key Distribution (QKD) network for metropolitan areas, resistant to quantum computing attacks and capable of supporting 800 Gbps data rates for mission-critical applications under real-world environmental conditions.

The research team demonstrated the ability of the newly developed QKD network to instantly detect and defend against eavesdroppers. It also studied the impact of realistic environmental factors on the quality of the quantum channel and used a QKD-secured optical channel to deploy and secure Link by J.P. Morgan, the world's first bank-led, production-grade, peer-to-peer blockchain network. This is the first demonstration of QKD securing a mission-critical blockchain application in the industry.

Under the leadership of JPMorgan Chase's Future Lab for Applied Research and Engineering (FLARE) and Global Network Infrastructure teams, researchers from all three organizations collaborated to achieve the following notable results:

- A QKD channel was multiplexed on the same fiber as ultra-high bandwidth 800 Gbps optical channels for the first time and used to provide keys for encryption of the data stream.
- Co-existence of the quantum channel with two 800 Gbps and eight 100 Gbps channels was demonstrated for a 70km fiber, with a key rate sufficient to support up to 258 AES-256 encrypted channels at a key refresh rate of 1 key/sec.
- Operation of QKD and the ten high-bandwidth channels was demonstrated for distances up to 100km.
- The proof of concept network infrastructure relied on Toshiba's Multiplexed QKD System, manufactured by Toshiba Europe at their Cambridge UK base, and Ciena's Waveserver 5 platform, equipped with 800 Gbps optical-layer encryption and open APIs running over Ciena's 6500 photonic solution. The tests were conducted in JPMorgan Chase's fiber optic production simulation lab.

"Security is paramount for JPMorgan Chase," said Marco Pistoia, PhD, Distinguished Engineer and Head of the FLARE Research group, JPMorgan Chase. "This work comes at an important time as we continue to prepare for the introduction of production-quality quantum computers, which will change the security landscape of technologies like blockchain and cryptocurrency in the foreseeable future. We are proud to be at the front-end of developing QKD technology for real-world applications while partnering with industry leaders in the field, such as Toshiba and Ciena."

At this time, QKD is the only solution that has been mathematically proven to defend against a potential quantum computing-based attack, with security guarantees based on the laws of quantum physics.

Steve Alexander, Chief Technology Officer, Ciena, added, "With more sensitive information being distributed across fiber-optic networks every day, robust encryption is of vital importance. As the quantum computing era approaches, research and development advances will continue to ensure the confidentiality of critical data as it travels over the network."

"Ciena has always pushed the boundaries of what is achievable with innovative network technology. We were the first to achieve 200 Gbps encryption, then first to obtain 400 Gbps. Now we are the first to offer 800 Gbps encryption to the industry. Working with forward-thinking companies like JPMorgan Chase and Toshiba is critical as we continue to build networking solutions to be more secure and efficient in supporting our digital world."

"Based on the success of this project we now have a proven and tested method for defending against quantum attacks on blockchain," said Yasushi Kawakura, Vice President and General Manager Digital Solutions Division, Toshiba America, Inc. "Toshiba is proud to contribute our QKD technology to this first-of-its-kind solution."

Suresh Shetty, Distinguished Engineer and Head of Blockchain Engineering for Onyx by J.P. Morgan, shared, "We are excited to have demonstrated that QKD can effectively secure communications between the various nodes in the Liink network against future quantum attacks."

8.Israel’s Microsoft of Quantum Computing Makes its Move

by Yonah Jeremy Bob
https://www.jpost.com/business-and-innovation/article-696832

Two days after the Defense Ministry announced a NIS 200 million commitment to building Israel’s first quantum computer, one of Israel’s leading quantum computing “software” companies, **Classiq**, announced an influx of $33 million in investment.

Classiq was founded in 2020 by Nir Minerbi (also CEO and former IDF Talpiot, 8200, and Rafael alumnus), Dr. Yehuda Naveh (also Chief Technology Officer and top academic) and Amir Naveh (also Vice President of R&D as well as former IDF Talpiot and Defense Ministry alumnus).

A statement from the company predicted that quantum computing will reach commercial maturity within only two years, even if some national security applications may take several years longer.

Eventually, it is anticipated that quantum computing will revolutionize military, economic and technological affairs and the basis for encryption of the entire Internet.

This has led the ministry, and more Israeli firms with former defense backgrounds like Classiq, to dive into the field to secure Israel’s place in one of this century’s premier tech-arms races.

In a visit to the company’s expanding offices in Tel Aviv, Classiq’s 30 employees, including a world-class development team in quantum computing, can be observed working with the high intensity of the fastest expanding start-ups.

The team comprises researchers holding advanced degrees from among the best universities in Israel and throughout the world, with nine alumni of the prestigious IDF Talpiot program and experienced senior software engineers.

Classiq plans to use the new funds to quadruple the size of the company – by opening new offices around the globe, hiring an additional 90 employees during the coming year and continuing to develop and file revolutionary quantum algorithm design patents.

The number of large organizations developing quantum software grew from 1% in 2018 to 30% in 2021 and is expected to continue to spike.

Giant companies, including the world’s large banks, pharmaceutical, automotive, energy, chemical, and cyber corporations, have created quantum computing teams that aim to develop software capable of generating benefits from quantum computers, said the press statement.

Classiq developed a “technological solution that facilitates a simpler way to develop quantum computer software, and allows people who are not necessarily quantum specialists to program this type of software."

The firm collaborates with technological giants such as Amazon, Microsoft, IBM, and Nvidia that are working to construct quantum computers.

The new funding round took place under the leadership of Phoenix, the venture capital arm of HPE, the investment arm of the Sumitomo Corporation (IN Venture), Spike Ventures, a Stanford University alumni investment fund and Samsung Next.

The current round also included personal investments from Lip-Bu Tan, current president and former CEO of Cadence, and Harvey Jones, CEO of Synopsys, and a board member at Nvidia.

Minerbi said, "the quantum computing revolution is in full swing. In recent years the vision is rapidly becoming a reality and is creating a real 'arms race' for constructing the quantum computer. Parallel to constructing the hardware led by the technological giants, Classiq is leading the world of software."

9.How Quantum Computing Could Transform The World

by Hans News Service
https://www.thehansindia.com/business/how-quantum-computing-could-transform-the-world-730021?infinitescroll=1

Quantum technology is one of the most researched areas and is attracting huge investments. This technology is having immense potential. This can be divided into **four verticals** — quantum computing, quantum communications, quantum sensors and quantum materials.

This technology is based on the phenomenon exhibited by particles like photons, electrons, etc. To describe the behaviour of these particles, quantum mechanics came into picture. The phenomena of Superposition, Entanglement, Teleportation (transfer of matter or energy from one point to other without travelling the physical space between them) and tunnelling (a phenomenon where a wave can propagate through a barrier) are exhibited by these particles. These aspects of quantum mechanics led to a number of interesting applications-exponential increase in computing power, inherently secure communication, interaction free measurements, precise and sensitive sensors, etc.

Classical computers have helped us unlock some mysteries, which we could not process with human power. They have been doubling in processing speed and computational power nearly every two years. This is known as Moore's law. But tasks such as quickly finding the prime factors for very large integers is out of reach for even the fastest conventional computer. The reason behind this is that finding the prime factors of numbers is a function that has exponential growth. Prime factorisation is the basis for secure types of encryption. Certain molecular modelling (to discover better drug treatment, understand our biology, etc) and mathematical optimization problems can crash any classical computer.

In the case of quantum computing, we will be able to take computing power to the next level. Quantum computers work by using quantum mechanical phenomena to process massive datasets where these datasets would bog down a classical computer. Researchers have a goal called Quantum Supremacy. Quantum supremacy is showing that any problem beyond the capabilities of a traditional computer can be solved on a quantum computer. The use of quantum properties such as superposition of states and entanglement speed up processing power and handle an unlimited number of variables.

Superposition

Classical computers are made up of millions or billions of transistors that exist in an 'ON' or 'OFF' state equal to 1 or 0 respectively. Quantum Computers use Qubits (quantum bits) that mimic the state of subatomic particles and can exist as a 1 or 0 or both at the same time. Whenever we measure its state, we will find that it is either ON or OFF. But between measurements, the quantum system can be in a superposition of both ON and OFF states at the same time.

Entanglement

Once two quantum systems interact with one another, they become entangled partners. The state of one system will give precise information about the state of the other system. This is known as entanglement.

Quantum computers, unlike the conventional computers, explore the full spectrum of possible computational solutions simultaneously, while classical computers look at each solution in sequence. In 2016 IBM made the first quantum computer with five qubits. In 2019 it was with 27 qubits. In 2022, it will be with 433 qubits. By 2023 Quantum computers with 1121 qubits will be built. As per New Moore's law, Quantum Volume doubles every year. Quantum Volume is the product of qubits added and error rate decrease. It is a metric that indicates the computational power of a quantum computer.

Quantum computing is a disruptive technology. People are excited about this technology. It has applications in cyber security, internet search and Artificial Intelligence. Almost every industry from finance to telecommunications can reap the benefits of Quantum computing. Lot of educational institutions have started courses on this subject. This technology has a lot of use cases in finance, agriculture, transport, etc. RBI can predict how their policies will affect the economy. It can be used to optimise investment portfolios. Improving nitrogen fixation can be achieved with better fertilisers minimising the pollution. The transport system can be overhauled. Better batteries can be designed with less charging time and with more life.

Initiatives of Government of India/Government institutes

The Government of India has taken three initiatives to promote Quantum technology.

This technology is research driven. Recognising this fact, the Department of Science and Technology (DST) through Quantum Enabled Science and Technology (QuEST) programme is conducting research in this field. Twenty one hubs and four research parks across India are participating in this programme. This programme is supported with a fund of 80 crore. About three hundred researchers are associated with this programme. To translate this research into product, DST has established an Innovation Lab in 2019 at Indian Institute of Science Education and Research (IISER), Pune with a budget of Rs 170 crores. To comprehensively address all the verticals in this crucial technology, India has launched the National Mission on Quantum Technology and Applications (NMQTA). This mission will scale up R&D and encourage translation of research and deployment activities. This initiative with a budget Rs8,000 crore spanning over the next five years will be led by DST. DST will coordinate with other stakeholders in carrying out this mission.

In 2020 DRDO demonstrated Secure Communications using QKD (Quantum Key Distribution) technology. QKD will address the threat that rapid advancement in quantum computing poses to the security of data being transported by the current communication infrastructure.

Recently Secretary, DOT inaugurated Quantum Communications lab at CDOT Delhi. Quantum Superposition, Entanglement and Teleportation provide exponential speedup over classical communications. He unveiled the QKD solution developed by CDOT which can support a distance of more than 100 Km on OF (Optical Fibre) cable. Indian Army has established a Quantum computing lab at Military Engineering Institute in Mhow, Madhya Pradesh. The research done at this lab will help the Indian Army transform its current system of cryptography to post quantum cryptography. Telangana Government is going to set up Quantum lab in association with Qulabs Software (India).

Way forward Though

India has become a software nation, we missed the bus in causing impact on making hardware in computing, telecom or any deep technology area. We should make the best use of the opportunity available now to become one of the world leaders in manufacturing the hardware for quantum computers. Demand for quantum skills is expected to grow at 135 per cent in five years. Lot of opportunities are there in this niche field. Quantum computing today is in that stage when classical computers were in 1944 (Vacuum tube based). A lot of quantum computing software is open source. Sectors such as manufacturing, banking and defence will likely lead in adopting quantum technology for critical applications. The ecosystem is growing. This technology will have use cases in all walks of life and a number of government agencies, academic institutions and start ups have built quantum computing use cases. Industry collaboration is required with academic institutions, and the government in adoption of this technology. Using quantum principles to compute is as different from classical computing as classical supercomputer is from abacus.

10.Biden's Cybersecurity Order Opens Our Post-Quantum Era

by Arthur Herman
https://thehill-com.cdn.ampproject.org/c/s/thehill.com/opinion/cybersecurity/594775-bidens-cybersecurity-order-opens-our-post-quantum-era?amp

The Biden administration has taken many hits for its policies, from the chaotic withdrawal of troops from Afghanistan to the highest inflation in 40 years to the humanitarian crisis at America's southern border. But last month, it scored a major success in getting the government's house in order in the cybersecurity domain and preparing the way for a safe and secure cyber future.

The White House has released a National Security Memorandum that, for the first time, focuses our national security concerns on the future threat of large-scale quantum computers to encrypted data, which means everything from government records and classified data to credit cards and banking transactions.

Instead of using digital bits to process data as a series of ones and zeros, as conventional computers do, quantum computers employ "qubits," which can represent any combination of 0 and 1 simultaneously. This allows computing power to grow exponentially as the number of qubits expands. A 2,000- to 4,000-qubit quantum computer, for example, can quickly decrypt almost all public-key encryption architectures - the ones used for everything from banking and credit cards to the power grid. Those architectures rely on numbers too big for conventional computers to factorize, but a quantum computer can and will do so.

Experts disagree on how soon we will see quantum computers of that size and capability. A recent RAND report says it might take 15 years; the CEO of Google, however, has stated publicly he thinks it could happen as soon as five or 10 years from now. One thing is clear: the one country that has the resources to do this besides the United States is China, the same regime that has waged cyber war on America and democratic states for two decades.

With this threat in mind, the White House has issued a landmark document, National Security Memorandum 8 (NSM-8), that pushes the government's cybersecurity into the post-quantum era: the first official step to making America's national security apparatus quantum ready and quantum safe.

The memorandum gave the National Security Agency 30 days to begin updating the Commercial National Security Algorithm Suite (CNSA), a process that will include adding quantum-resistant cryptography, CNSA being the collection of secure algorithms approved for use by all encrypted data users, including the private sector.

Within 180 days, agencies that handle national security systems are supposed to identify any and all "instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms," or the updated CNSA, and to draw up "a timeline to transition these systems to use compliant encryption, to include quantum resistant encryption.”

This document is the first I'm aware of coming out of the White House national security apparatus that specifically mentions quantum-resistant cryptography in the context of current federal cybersecurity planning. That's a big victory for our Quantum Alliance Initiative here at Hudson Institute, which has been pushing the quantum security issue for the past four years, and for quantum information science generally.

At the same time, it's important to realize the next and most vital step is execution.

Here's where Congress has to step up, with oversight, funding and making sure that what needs to be done to confront a future quantum security threat gets done. That includes demanding a full briefing from the White House for key congressional committees, along with other federal agencies, on what the implications of NSM-8 are for our nation's cyber future.

In the final analysis, we are going to need an all-of-government approach to dealing with the gravest cybersecurity threat of this generation - indeed, the greatest threat of this century.

This is particularly true for alerting the private sector, including our financial services sector and corporate sector where replacing the RSA-based systems will require years of work and continual updating. The preliminary study we've done at the Quantum Alliance Initiative estimates that a single quantum attack on one of the five largest financial institutions in the U.S. disrupting access to the Fedwire Funds Service payment system would cause a cascading financial failure costing anywhere from $730 billion to $1.95 trillion. Indeed, a quantum computer attack could impair nearly 60 percent of total assets in the banking system because of bank runs and endogenous liquidity traps.

Given the fact that the federal government finally admits this is a security threat grave enough to demand action from agencies within the next five months, that's all the more reason why private industry needs to take this threat seriously - and to insist that Washington to put together a comprehensive plan to protect all of us from future quantum attack.

11.Cryptographic Agility: Exploring Proxy Approaches

by David Ott, Sean Huntley, Mark Benson
https://octo.vmware.com/cryptographic-agility-exploring-proxy-approaches/

Enterprise security teams are increasingly aware of post-quantum cryptography (PQC), which is actively being standardized by the National Institute of Standards and Technology (NIST). At some point, PQC protection from the threat of scaled quantum computers will become a regulatory requirement, rather than a fuzzy future concern on a long to-do list.

But how will an enterprise get to the deployment finish line in the PQC challenge, when it is common to have hundreds — even thousands — of software applications and services that will require migration?

To say that this process will be complicated is a vast understatement. Many enterprises purchase most (or all) of their software from external vendors. Each supplier will need to manage the changes and make the resulting configuration options available to customers. One would expect a great deal of diversity in rates of migration and readiness across vendors. Working with so many individual suppliers will be daunting, to say the least. No doubt, there will be applications that will be slow (or impossible) to migrate because of underlying legacy components.

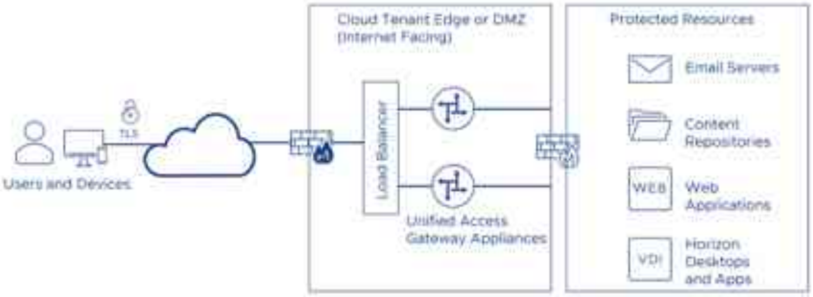
For enterprises that develop applications and services for in-house and customer use, development teams will have to examine the technical challenges and put the work on the development roadmap. It won't take long, however, before exploratory work reveals dependency challenges, such as the availability of PQC libraries, open source components, component services (e.g., databases), systems software, and domain-specific standards specifications. Significant changes in PQC key sizes, memory and computation requirements, and communication patterns will also complicate implementation. Yet another thing to navigate will be hybrid configurations that combine cryptographic algorithms — something few software stacks are designed to accommodate.

What would help at the outset is a framework for cryptographic agility that is somehow decoupled from individual applications and can be deployed in advance of the software industry's heavy lift of migrating myriad applications to PQC standards. Such a scheme could reel in the crypto migration challenges to a single software domain on behalf of many other applications and provide early quantum safety before established solutions can be worked out and deployed more widely.

Considering proxies as a solution

One way approach to PQC migration — and cryptographic agility more broadly — would be to use proxies. In the context of distributed applications, proxies introduce an intermediary node between two communication endpoints. In particular, our interest is in reverse proxies, which are often installed on an enterprise network at the demilitarized zone (DMZ) or at a cloud tenant edge, to manage incoming client connections to backend application services. Reverse proxies are used for a variety of functions, including load balancing, content caching and translation, application firewalls, authentication, authorization, and compression. In this case, we are interested in Transport Layer Security (TLS) termination and the opportunity to modify the cryptographic algorithms used in secure communications over the Internet.

An illustrative case study is VMware's Unified Access Gateway (UAG), a specialized reverse-proxy virtual appliance deployed in a cloud tenant network or enterprise DMZ network in a standalone or load-balanced configuration. It is typically Internet-facing and manages authentication and authorization of incoming TLS connections to securely access VMware Horizon desktops and applications, as well as other enterprise resources. UAG runs on VMware vSphere, Amazon AWS EC2, Microsoft Azure, and Google Cloud GCE. The uses for UAG are too numerous to list but include both cloud-based services (such as access to virtual desktops and published apps, web applications, content repositories, and email) and edge-based services (such as secure content gateways, VPN services, web reverse proxying, identity bridging, and Horizon-based applications).



High-level UAG Deployment Architecture

A key customer requirement for UAG is compliant configurations for regulatory standards-based deployments. Some of the most important include PCI DSS 3.2.1, HIPAA, NIAP/CSfC, FedRAMP, and NIST SP800-52. Such standards dictate permissible TLS versions (1.2 and/or 1.3), cipher suites (public key, symmetric key, cryptographic hash), acceptable elliptic curves, OCSP Stapling, and specific TLS options. UAG customers often test compliance with third-party tools, such as ImmuniWeb and Qualys/SSLLabs, and have come to expect an "A+" rating.

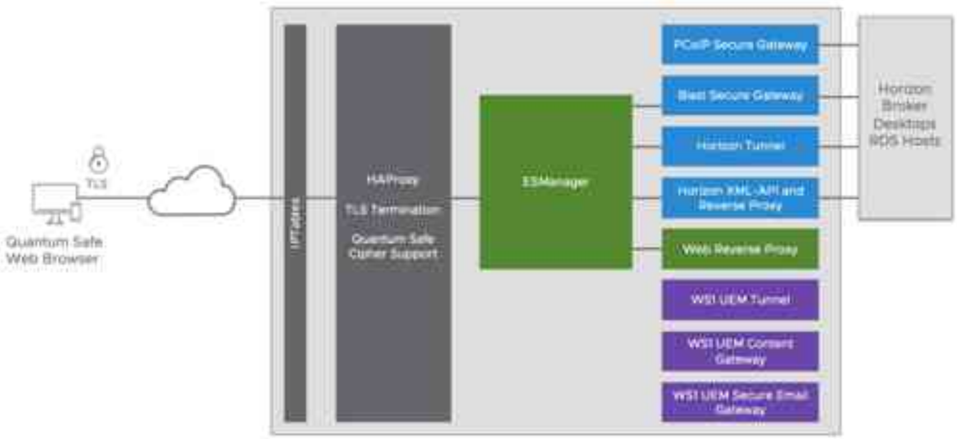
A key problem in UAG support for PQC is the large number of backend applications that would require migration. Another key challenge is preparing for the migration in a way that facilitates subsequent changes (in case NIST standards are later revised). Another key requirement is that changes to cryptographic algorithms should not require rebuilding the application. This ensures rapid uptake of security patches and ongoing configuration changes. Finally, if possible, the solution should avoid major refactorization of UAG as a stable software architecture.

With a single proxy component, we can enable quantum-safe cryptography across public networks on behalf of the many backend applications communicating through UAG. The proxy component may be designed to support an extensive range of cryptographic algorithm configurations and the use of libraries not supported by the underlying services. Meanwhile, communication between services can continue to use existing cryptography capabilities, since communications take place behind a firewall.

A UAG case study in cryptographic agility

UAG's architecture includes a large number of backend components. As seen in Figure below, many of these services are managed by the edge service manager (ESManager). In front of these components is HAProxy, which offers forwarding features after server name indication (SNI) header inspection — for example, TCP 443 port sharing.

Our exploratory prototype of cryptographic-agile UAG leverages HAProxy's ability to segment secure communication by terminating TLS at the proxy and then using a second TLS connection to each backend service. This creates a single implementation and configuration point for cryptographic agility. A key insight here is that quantum safety is needed across the Internet path between a client device and UAG, but not necessarily between UAG and a backend service communicating within the same private network.



Cryptographically Agile UAG Architecture

Reconfiguration of HAProxy allows for rapid changes in supported TLS ciphers and other parameters. Furthermore, by storing pre-compiled cryptographic library modules — each configured to use different cryptography — the UAG team can easily change cryptographic implementations. Supporting new cryptography only requires updating one component.

Our work on quantum safety for UAG makes use of the Open Quantum Safe (OQS) implementation of PQC candidate standards. OQS is an open source project pioneered by the University of Waterloo and industry collaborators. It is intended to make NIST PQC implementations available for experimentation and testing. In particular, liboqs provides a C library that integrates PQC with various protocols and applications, including OpenSSL.

For more on our crypto-agile implementation of UAG, see a short preview of our VMworld 2021 session and read the associated blog.

Final thoughts

Proxies are a powerful approach to enabling cryptographic agility (including quantum safety) for myriad supplier applications and services. By decoupling cryptographic configuration from individual applications, it offers the following advantages:

- Facilitating early PQC support for a large number of applications that may otherwise be slow to migrate as a collective
- Serving as a central point of enterprise cryptography configuration and management

- Providing a way to quickly address vulnerability remediation and/or ongoing PQC standards change

- Addressing cryptographic agility at scale within sizable enterprise infrastructures

Our experimentation with the Unified Access Gateway, as part of VMware's Horizon software suite, has provided a testing ground for cryptographic agility and PQC migration within a widely adopted VMware product. The reverse proxy architecture supports cryptographic library extensibility and the ability for enterprise customers (and VMware itself) to create standards-compliant configurations that are scalable for many backend enterprise applications.

12.Meet Twist: MIT's Quantum Programming Language

by Rina Diane Caballar
https://spectrum.ieee.org/quantum-programming-language-twist

A team of researchers at MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) have created Twist, a new programming language for quantum computing. Twist is designed to make it easier for developers to identify which pieces of data are entangled, thereby allowing them to create quantum programs that have fewer errors and are easier to debug.

Twist's foundations lie in identifying entanglement, a phenomenon wherein the states of two pieces of data inside a quantum computer are linked to each other. "Whenever you perform an action on one piece of an entangled piece of data, it may affect the other one. You can implement powerful quantum algorithms with it, but it also makes it unintuitive to reason about the programs you write and easy to introduce subtle bugs," says Charles Yuan, a Ph.D. student in computer science at MIT CSAIL and lead author on the paper about Twist, published in the journal Proceedings of the ACM on Programming Languages.

"What Twist does is it provides features that allow a developer to say which pieces of data are entangled and which ones aren't," Yuan says. "By including information about entanglement inside a program, you can check that a quantum algorithm is implemented correctly."

One of the language's features is a type system that enables developers to specify which expressions and pieces of data within their programs are pure. A pure piece of data, according to Yuan, is free from entanglement, and thereby free from possible bugs and unintuitive effects caused by entanglement. Twist also has purity assertion operators to affirm that an expression lacks entanglement with any other piece of data, as well as static analyses and run-time checks to verify these assertions.

To evaluate the language, the team wrote programs in Twist for a set of well-known quantum algorithms and executed them on a quantum simulator. "We performed experiments that showed the overhead of running these runtime checks is no more than 3.5 percent over running the base program, which we believe is fairly low and a good trade-off for the safety guarantees the language gives you," Yuan says.

The team also introduced small bugs to some of the programs and found that Twist can detect those bugs and reject the erroneous programs. "We hope that when people use our language or design new quantum languages for their specific use cases, they'll be able to look at our work and say that the idea of purity and having entanglement as a feature is something they want because it will give them more confidence that their programs are correct without having to run a lot of expensive simulation and testing," says Yuan.

While many researchers are focused on building efficient and optimized quantum hardware, Twist aims to fill the gap in quantum software. "Drawing some parallels to what we're seeing with machine learning and other high-performance computing applications—where with every new phase of hardware development we get a new system and potentially new capabilities— there are perhaps many incredible opportunities to be had by harnessing the hardware. But it almost always is the software that stands in the way of people having access to that hardware and being able to deploy it and use it widely in different software systems," says Michael Carbin, an associate professor at MIT and coauthor of the paper about Twist. "A lot of the work we're doing is laying some of the foundations and trying to tease out what some of the core abstractions are that may make these types of devices more programmable."

Yet one of the challenges the team faced in building Twist is the lack of a standard for what quantum programs should look like. "Over the years, people have developed core algorithms to solve individually complex tasks like factoring integers, but it's less clear how we can build an entire ecosystem of software for it," Yuan says. "With Twist, we were able to build the language around our best consensus of the tasks we want to perform on quantum computers and make it as expressive as possible for those tasks."

In terms of limitations, Twist can only tell you whether or not a piece of data is entangled with other pieces of data, but not how they're entangled. "The exact way they're entangled is what will determine whether a quantum algorithm is correct, but there are an infinite number of ways in which data can be entangled," says Yuan. "It's a real challenge to be able to give that finer-grained detail, and it's something we'll need to do in the future."

The team is now working on another language that builds upon Twist to tackle other quantum phenomena such as phase and superposition, but they hope Twist will pave the way for creating better quantum programs.

"For a developer trying to implement a quantum algorithm, they need the tools built into the language to tell them something is happening in their program that's caused by entanglement," Yuan says. "If we can build core language principles and features that allow a developer to reason about entanglement, we can make it so entanglement is less of a cognitive burden, and allow developers to write more intuitive programs."

13.China Releases New Quantum Computing Software

by CGTN
https://news.cgtn.com/news/2022-02-18/China-releases-new-quantum-computing-software-17KawSS-F1Qc/index.html

China has released a new quantum computing programming software named "**isQ-Core**" and deployed it to the country's superconducting quantum hardware platform.

It represents a significant step forward in the combination of home-grown quantum computing hardware and software, said its primary developer, the Institute of Software under the Chinese Academy of Sciences.

According to the institute, the isQ-Core has the advantages of simplicity, ease-of-use, high efficiency, solid scalability and high reliability.

It will provide support for scientists to conduct quantum computing theory and application research, said the institute in a statement Thursday.

China has achieved rapid quantum computer development, with the launches of "**Jiuzhang,**" "**Zuchongzhi**" and "**Zuchongzhi 2**" in recent years. Similar to conventional computers, quantum computers also need software to manage hardware devices, run applications and provide a user interface.

Researchers announced that they have deployed isQ-Core on a CAS quantum computing cloud platform, currently the largest in China in terms of hardware scale.

14.JPMorgan Chase Readies For Post-Quantum Security World

by Nicole Hemsoth
https://www.theregister.com/2022/02/17/jpmorgan_postquantum/

These days it seems every major company is outlining a quantum strategy, even if those plans are nebulous at best. However, in areas like financial services, especially at global banks like JPMorgan Chase, getting a handle on both quantum computing and quantum security are top priorities.

It all boils down to the next generation of secure transactions. As the reliability and capability of quantum computers expands those systems are more prepared to crack traditional modes of securing encrypted data. The best defense in this post-quantum security world are quantum communications and specifically, quantum key distribution (QKD).

Think of quantum communications as two parties agreeing on the same key using photonic-based quantum technology. Those parties agree on a key by measuring particles as they lose fidelity. As the distance increases between the two servers and particles break it becomes impractical to get them to agree on the same key, so getting distances ever-longer is one of the most pressing challenges when it comes to post-quantum security.
Spearheading this effort is Marco Pistoia, distinguished engineer and head of the Future Lab for Applied Research and Engineering (FLARE) at JPMorgan Chase. Pistoia jumped to the bank after a 24-year career at IBM Research where he focused on security.

He spent the early decades of his career working on static program analysis for security (analyzing programs without executing them, something that sounds easy but is exponentially complex and takes quantum-class resources to do for practical use). He then moved into quantum algorithms and noticed that JPMorgan Chase was leading the way in future quantum security.

As Pistoia tells The Register, "This is technology that is solid and provably secure," but we are several years from seeing the impact in terms of security even in the most forward-looking banking environments. "With quantum key distribution (QKD), maybe it will be a hybrid solution with post-quantum cryptography and QKD but the impact of this combination will be very reliable, secure networks we can use confidently, especially in financial institutions where we run very delicate transactions."

JPMorgan Chase is watching quantum computing for the emerging threat quantum hacks present but for the real work, it's all about long-distance QKD.

"When it comes to security, the QKD boxes that generate keys from different parties are already available, so in our experiments that's what we used to get the 100km distance. Two parties still have to be relatively close to each other, which is good for metro areas but we need much longer distance QKD for it to be operational and have an impact," Pistoia tells us.

On that point that this is all future-focused, one of the non-technical (in terms of qubits or algorithms) to arriving at post-quantum security is the National Institute of Standards and Technology (NIST). JPMorgan Chase is waiting on (and working with) NIST to provide recommendations about the algorithms that should be used. "But this is time that should be used in an intelligent way," Pistoia explains.

"We need to start to identify where the vulnerable parts of a network are in company infrastructure and those should be captured in a database so when recommendations from NIST are ready we know exactly what need to address in hardware, software, and most challenging, in third party components."

- IBM forges entanglement to double quantum simulations by 'cutting up a larger circuit into smaller circuits'
- D-Wave to go public after $1.2 billion merger deal with SPAC
- Quantum computing to grow by 50 per cent per year until 2027, when revenue will still be chump change
- Baidu's AI predictions for 2022: Autonomous driving! Quantum computing! Space! Human-machine symbiosis!

Under the leadership of JPMorgan Chase's Future Lab for Applied Research and Engineering (FLARE) and Global Network Infrastructure teams, researchers from all three organizations collaborated to achieve the following notable results:

- A QKD channel was multiplexed on the same fiber as ultra-high bandwidth 800 Gbps optical channels for the first time and used to provide keys for encryption of the data stream
- Co-existence of the quantum channel with two 800 Gbps and eight 100 Gbps channels was demonstrated for a 70km fiber, with a key rate sufficient to support up to 258 AES-256 encrypted channels at a key refresh rate of 1 key/sec.
- Operation of QKD and the ten high-bandwidth channels was demonstrated for distances up to 100km.
- The proof of concept network infrastructure relied on Toshiba's Multiplexed QKD System, manufactured by Toshiba Europe at their Cambridge UK base, and Ciena's Waveserver 5 platform, equipped with 800Gbps optical-layer encryption and open APIs running over Ciena's 6500 photonic solution. The tests were conducted in JPMorgan Chase's fiber optic production simulation lab. On the research block now are technologies that sound familiar from the good old Wi-Fi days: repeaters, for instance or more future-focused, trusted nodes. In short, there's still a long way to go.

Luckily, for at least the next couple of years, there's time. But mounting qubit counts and reliability along with quantum algorithm advances could push us into the world of post-quantum security before we're ready. It's better to be first to security than first to found out the old ways don't work without notice.

"What we'll see in the next couple of years is more companies will start to look closer at post-quantum cryptography and quantum key distribution. This seems to be the strategy for the future. To protect the confidentiality and integrity of data, it's good to start migrating now, even if quantum computing is years away. It's important to be proactive about this," he adds.

15.Infineon IC Addresses Post-Quantum Security

by David Manners
https://www.electronicsweekly.com/news/business/infineon-ic-addresses-post-quantum-security-2022-02/

Infineon has brought out a chip for post-quantum cryptography (PQC) using XMSS signatures called OPTIGA TPM (Trusted Platform Module) SLB 9672.

This mechanism counteracts the threat of firmware corruption by attackers with access to quantum computers and increases long term survivability of the device by enabling a quantum-resistant firmware upgrade path.

The standardised, out-of-the-box TPM provides a solid foundation for securely establishing the identity and software status of PCs, servers, and connected devices, and for protecting the integrity and confidentiality of data at rest and in transit.

Infineon's latest addition of the OPTIGA TPM family is the industry's first TPM to offer a firmware update mechanism with a 256-bits key length, along with an additional check based on PQC.

With this update mechanism, the OPTIGA TPM SLB 9672 can still be updated if the standard algorithms are no longer trusted.

Its design is engineered for improved computing performance with fail-safe features that counteract the effects of corrupted firmware. For instance, built-in fail-safe features enable TPM firmware recovery in accordance with the NIST SP 800-193 Platform Firmware Resiliency Guidelines.

This TPM also provides an expanded non-volatile memory to store new features such as additional certificates and cryptographic keys.

Security evaluation and certification are performed by independent bodies according to the Common Criteria and FIPS requirements.

The TPM   fully complies with the Trusted Computing Group (TCG) requirements (TPM 2.0 standard version 1.59) and is certified according to the latest TPM 2.0 standard.

Featuring a standardised trust base, as well as various tools to support design activities (software/demo boards), this TPM enables easy integration with host software. It also supports the latest versions of Windows and Linux. Furthermore, the chip boasts an extended temperature range of -40°C to 105°C.

Infineon is committed to the long-term availability of OPTIGA TPM SLB 9672 for a minimum of ten years and offers tailored support and maintenance through the Infineon Security Partner Network (ISPN). With this long-term commitment, customers can not only rely on the TPM's continued availability but also on Infineon's support.

16.Quantum Cryptanalysis: Hype And Reality

by Chris Jay Hoofnagle, Simson Garfinkel
https://www.lawfareblog.com/quantum-cryptanalysis-hype-and-reality

In 1994, Peter Shor fired the starting gun of the quantum computing race. Shor found that a quantum computer — in those days, a device only imagined by physicists and theoretical computer scientists — could solve a math problem that in turn would make it possible to efficiently factor large numbers. Because much of modern encryption depends on the assumption that such factoring is too time-consuming for even all the world's computers working together to crack a single key, Shor's insight led to massive public and private investment in quantum computing. Inadvertently, it also caused many observers to view quantum computing mainly as a threat to encryption.

Today, nation-states and even private companies compete for "quantum computing superiority," a quantum computer that is so fast that it can solve problems that cannot be realistically solved by classical computers (the kinds of computers that we use every day). The United States, China, the European Union, and individual European nations (France, Germany, the United Kingdom) are pumping billions into the field. And make no mistake: Quantum computers are here today. They just aren't very powerful for solving real-world problems like factoring or revealing the secrets of photosynthesis.

Nevertheless, the public can now purchase shares in IonQ Inc., a pure-play quantum computing company that is listed on the New York Stock Exchange through the controversial but increasingly common practice of using a SPAC (special purpose acquisition company). And even relatively small startups have working, yet equally small, quantum computers. Chinese scientists can credibly claim to lead the quantum computing race, with peer-reviewed publications in top journals detailing their technical might. One of the Chinese machines even claims "quantum supremacy," although it is supremely capable of solving a problem that is of no practical interest to anyone but quantum computing researchers and their investment bankers.

Does this mean that society is on the verge of losing all of its secrets to quantum cryptanalysis — possibly to a single geopolitical actor, like China? We confidently assess that this is improbable. Quantum cryptanalysis may indeed be a threat in the distant future, but we believe that the cryptanalytic usefulness of quantum computers will be limited, if they are possible at all. Here we highlight technical, practical, and economic and strategic reasons why cryptanalysis is a boogeyman. Cryptanalysis has occupied too much of the spotlight on quantum computing. That spotlight casts shadows on different, more realistic risks and benefits.

The State of the Science

Quantum computers are here today, both in research labs and in production. But even today's most performant devices — the laboratory trophies that are at the very bleeding edge of what is possible with today's technology — are far from leveling attacks on public key encryption systems like RSA. Scientists have made steady progress, but not enough to be a realistic threat.

Whereas modern computers are measured in bits and bytes — your new cell phone probably has a 64 — bit processor and perhaps 256 megabytes of storage — quantum computers are measured in qubits. Although many popular accounts of quantum computers say that qubits simultaneously have the value of 0 and 1, that's not strictly true. Instead, qubits can have a value of either 0 or 1, but the value isn't determined until the end of quantum computation. Whereas conventional computers consist of circuits that process data, quantum computers are more properly thought of as a collection of indeterminate data — qubits — that experience a program: at the end of the program's execution, each qubit is measured. Typically a program must be played multiple times with many separate measurements before the outcome of a computation can be known with high accuracy.

In 2001, a 7-qubit bespoke quantum computer constructed by Isaac Chuang's group at IBM Almaden Research Center successfully factored the number 15 into its factors 3 and 5. The number 15 is represented in binary by four bits: 1111. The number 15 is also, not coincidentally, the smallest number that is not prime, not even, and not a perfect square. So realistically, it's the smallest number that the IBM team could have meaningfully factored. The "quantum computer" was based on a chemical that had been specially synthesized to have 7 qubits.

Since IBM's demonstration, other researchers have factored larger numbers on quantum computers. None of these approaches has managed to factor a number out of reach of a conventional computer. Most of the numbers factored can be factored with pen and paper. For example, in 2012 a team led by Nanyang Xu at the University of Science and Technology of China, Hefei, successfully factored the number 143.

More recent examples that have captured public attention include a January 2019 factoring of the 7-digit (20-bit) number 1,005,973 using a special kind of quantum device known as an annealing machine. This was an exciting development because it was previously thought that annealing quantum computers could not factor. This seemed to expand the cryptanalysis threat. The scientists reasoned that because the manufacturer of the device scaled it dramatically in just seven years, perhaps a machine capable of factoring the kinds of numbers used to secure today's commercial internet might be constructed in years, and not in decades.

The current record described in the peer-reviewed literature factors a 13-digit number, 1,099,551,473,989.

For comparison, credible estimates predict that quantum cryptanalysis will require a large machine, one far bigger than anything built today, and one with far fewer errors. Instead of factoring 7- or 13-digit numbers, an attacker will need to factor 300-digit ones. A National Academies group assessed in 2019 that cryptanalysis against a weak RSA-encrypted message "requires building a machine that is more than five orders of magnitude larger and has error rates that are about two orders of magnitude better than current machines[.]" Google scientists estimated that factoring a conventional RSA public key in use on the commercial internet today "would take 100 million qubits, even if individual quantum operations failed just once in every 10 000 operations." That article was titled "Commercialize Quantum Technologies in Five Years" and was published in 2017. In 2022, the largest quantum computer has just 127 qubits.

Quantum Computing Is Only a Threat to Modern Public Key Cryptography

When commentators predict a collapse in encryption, they are describing attacks against systems based on public key cryptography, such as RSA using the Shor algorithm (a method for using quantum computing to find a number's factors). The statistics we relate above focus on RSA attacks.

Public key cryptography is rarely used by itself in modern computing systems. Instead, a public key is used to encrypt Advanced Encryption Standard (AES) encryption keys: It is the AES keys that are used to encrypt the actual email messages, web pages, banking transactions, and bulk data on a hard drive. If you have an iPhone, its data is encrypted with AES.

In 1996, Lov Grover came up with a way to use a performant quantum computer to significantly cut the time that it takes to search for an AES encryption key. With Grover's algorithm and exclusive use of a quantum computer, it might be possible to crack a 128-bit AES key in somewhere between 5 hours and a year, depending on many details. That's why many governments and manufacturers have been upgrading their systems from AES-128 to AES-256. The upgrade, which is essentially cost-free, puts AES cracking out of range for even the most imaginably advanced quantum computer using today's cryptanalytic methods.

Of course, there might be a breakthrough in the underlying cryptanalytic methods themselves—or in the understanding of complexity theory on which they are fundamentally based. If computer scientists ever discover that P=NP, then attacking encryption algorithms like RSA-2048 and AES-256 could become the stuff of high school science fairs soon thereafter. If P=NP, then computer scientists would be able to find fast and easy solutions to nearly all of today's difficult problems. Today, most computer scientists do not think that we live in a world where P=NP.

The Practical Realities of Cryptanalysis

Some commentators who discuss quantum computing imply that the mere existence of a large machine would undo all encryption. Like in the 1992 movie Sneakers, they suggest that successful quantum computing would unravel the world's secrets in an automatic way, perhaps by finding some fundamental weakness in all encryption systems. But this is not the case. Instead, the attacker will have to use the quantum computer for cryptanalysis on a key-by-key basis. And even then, attackers would be able to decrypt only those messages that they had successfully intercepted and stored. This leads to three practical challenges that set bounds on the quantum cryptanalysis threat.

- **First, the attacker must acquire the encrypted data to analyze** — meaning the attacker needs some kind of surveillance capacity against the target. The quantum cryptanalysis threat actor, therefore, comes from nation-states with large surveillance and storage capabilities, and from private actors with particular dominance on the internet. The biggest risk comes from institutions with the resources and incentives to keep messages for decades.

- **The second challenge is time**. Cryptanalysis, even on a quantum computer, will take a lot of time. The National Academies estimated that a strong RSA key would take 28 hours to crack, while a 2019 Google paper proposed a method that would require 8 hours. Even a standard 2,048-bit key is projected to take 3.5 hours to crack.

- **The third challenge would be resource management**. Military doctrine envisions a process involving targeting, tasking orders, and deconfliction for making such rationing decisions. Targeting is the process of selecting and making a priority of messages and pairing an appropriate response. Once targets are chosen, a military command would issue a tasking order to choose a method to attack the message.

To illustrate why this process is important, consider an organization that can intercept wireless messages between a target's phone and a publication service such as Twitter. Each wireless message might contain a tweet destined for immediate publication, a tweet scheduled to be published at some point in the future, a direct message to another user, or perhaps a status check, polling the service for other messages posted by other users. Some of these messages are clearly more valuable than others, but they all require the same level of effort to decrypt.

And here is the problem: With a well-designed encryption system, there is no obvious way to differentiate among messages before one is decrypted. Encrypted messages are easy to create, so a smart adversary can generate many worthless ones to flood or overwhelm another state's capacity to decrypt. Lengthening keys imposes more time requirements on the attacker as well. The National Academies estimates that those using an 8,000-bit RSA key would impose 229 hours (about 1 and a half weeks) of work on the attacker.

Twitter is a relatively public service, yet it still presents challenges for analysis. The situation is more challenging in other contexts because of advances in cryptographic features. Strong encryption has been available since the 1990s but has only recently become ubiquitous and usable. Today, however, strong encryption is everywhere, and modern systems implement forward secrecy, so that the compromise of one key will not endanger the secrecy of other messages.

The term "**deconfliction**" describes systematic management procedures to coordinate the use of resources by various stakeholders. Quantum cryptanalysis will require multiple layers of deconfliction. At the most basic level, there will need to be an equities process to decide who gets to make the decisions.

Targeting and resource prioritization will become significantly more complex if the very existence of the quantum cryptanalysis system is itself a state secret. Policymakers will need to decide whether the results from cryptanalysis can be exploited directly, or if the results will need to be closely held to prevent adversaries from learning the extent of the organization's cryptanalytic capabilities.

What do these challenges mean in full? "Key value" emerges as an important factor. Attackers will need to focus on high-value keys—such as developer certificates—that give the attacker access to entire devices or services. Conversely, smart defenders will consider the time-value of their secrets and invest in defending the most important keys.

Meanwhile, the window of vulnerability is closing rapidly, as work is underway to choose and deploy post-quantum cryptography systems that will likely be resistant to attack from even a large, reliable quantum computer. Deployment of such systems will take years and coordination, similar to the upgrade from AES-128 to AES-256. But in the meantime, there are relatively simple and inexpensive countermeasures: lengthening keys, choosing forward-secrecy-enabled services and using AES where possible.

The Economic and Strategic Reality of Cryptanalysis

The economics and strategy of quantum technologies reveal cryptanalysis to be a minor concern; this is unfortunate because the spotlight on cryptanalysis leaves other uses of quantum computing in the shadows.

The quantum computing race differs from prior big-science projects because of the role of the private sector. It is plausible that a technology powerhouse like IBM or even a startup in the field may develop the first strategically significant quantum computer. But no matter who develops that device, they will almost certainly be smart enough to not waste its capabilities on cryptanalysis.

Relatively speaking, there is not much money to be made in cryptanalysis. Realistically, governments are the only real buyers of the service. While governments have deep pockets, other uses of quantum computers are more strategic and remunerative.

The smart strategy will be to use one's quantum computer to build ever-bigger quantum computers. Indeed, companies in quantum computing identify chemistry and materials science as their research focus. This is because with a mid-scale quantum computer, one might discover fundamental insights in materials design and in chemistry that elucidate strategies to build a larger quantum computer.

Thus, like classical computers before it, quantum computer strategy is to trigger a virtuous cycle of growth. This insight also foreshadows an innovation policy issue: Groups that can make those fundamental observations are likely to pull ahead of the pack, building ever-larger computers with teams that were trained over decades, using discoveries that competitors cannot obtain. In this large-scale scenario, quantum computing could be a winner-take-all technology, suggesting that the first innovator might well become the most successful one.

In addition to the potential winner-take-all prize, the focus on quantum chemistry and materials science could lead to fantastically remunerative scientific discovery. Priorities include better understanding photosynthesis, nitrogen fixation, and the development of new pharmaceuticals. Innovations in those fields will mint untold billions and create entire new economic realities. Viewed in this light, using a quantum computer for cryptanalysis will be like developing satellites for surveillance and never allowing them to be used for weather or civilian communications.

What the Public Should Be Worried About

Dramatic claims about the capabilities of quantum computers may be driven by marketing, wishful thinking and even strategic considerations. Marketing and wishful thinking are easy to understand: Companies want to position themselves as unparalleled leaders in the quantum computing field. The strategic considerations are more important and serve a political end: to quell concerns that might lead to regulation.

Inevitability is one moat against regulation. By making dramatic claims, such as, "in a 5 to 10 year timeframe, quantum computing will break encryption as we know it today…," companies suggest that social regulation is impossible because the realities of the technology will make them futile. Such claims are the acceptable, modern equivalent of "you have zero privacy anyway. Get over it."

The second strategy is to elide military applications of quantum technology. Just as with artificial intelligence, some will hand-wave with far-off promises instead of focusing on who is funding quantum technologies and why.

Obscured in the shadows of cryptanalysis are far more anti-social uses of quantum computers. Optimizing the fixation of nitrogen may also lend insights into more destructive nitrogen bombs. Chemical discovery could lead to new kinds of chemical, biological and even genetic weapons.

A huge portion of government expenditure in quantum technologies envisions new sensing systems for intelligence and war fighting. Indeed, quantum sensing will provide exquisitely sensitive devices, ones that could create entirely new surveillance capabilities with few countermeasures.

The privacy threat from quantum technologies—at least in the near term—comes from quantum sensing that will give some actors the ability to sense gravity and electromagnetic fields remotely and through natural barriers such as walls and roofs. Quantum devices that increase the precision of measuring time will provide more resolution to other kinds of sensing as well. The real privacy threat we face is that quantum-capable governments and companies will be able to sense more and, thus, know more about us.

The strategic threat comes from reducing the stealthiness of submarines and low-observable aircraft. Imagine a world where a single, quantum-superior government can see all other nations' weapons systems and critical infrastructure from space.

Conclusion

In sum, quantum cryptanalysis is a threat, but one that we consider to be overhyped. Simply put, quantum computers will not magically break all encryption quickly, as sometimes implied by the news media and even by some policy analysts. Instead, attackers will carefully choose and focus their cryptanalysis resources on high-value keys, presumably ones that cannot be attacked using other intelligence tradecraft.

The collapse of encryption has captured the attention of the media and led to many privacy doomsday predictions about quantum computers. This narrative is unfortunate, because we believe that quantum computing has both more strategic opportunities and more positive potential for society through the application of quantum simulation.

17.Quantum Errors Made More Tolerable

by Julien Levallois
https://www.swissquantumhub.com/quantum-errors-made-more-tolerable/

In modern computing devices, literally billions of transistors work restlessly in almost perfect harmony. The keys to producing near-perfect computation from devices made from imperfect components are the use of digitisation and error correction, with the latter encompassing procedures to detect and rectify inaccuracies as they occur. The challenge of preventing errors from accumulating is one that future quantum computers have to face as well — in fact it forms the main barrier to realizing useful computations. Alas, the tools that have been perfected for classical computers cannot be applied directly to quantum computers, which play by another set of rules, those of quantum mechanics. Ingenious solutions for quantum error correction have been proposed over the past couple of decades, and recently there has been encouraging progress towards implementing such methods in state- of-the-art quantum computers. Writing in Nature Physics, the group of Prof. Jonathan Home at the Institute for Quantum Electronics report such an experimental realization — one that stands out by factoring in important limitations of physically realistic devices and by being relatively easy to implement compared to other proposed error- correction schemes, thus increasing the relevance of the demonstration for practical quantum computation.

Allowing a quantum of error

The way information is processed in quantum computers differs fundamentally from that in their classical counterparts. This opens up unique computational capabilities, but also calls for novel strategies to deal with errors that occur in the process. More specifically, quantum information cannot be perfectly duplicated, and measurements inevitably alter the fragile quantum states. Nevertheless, with some creative rethinking it is possible to devise measurements that can tell us whether the quantum information has been disturbed. As with classical error correction, the key is to harness redundancy.

Among the innovative ideas that have emerged for quantum error correction, the so-called Gottesman–Kitaev–Preskill (GKP) code is a particularly promising one, using flexible control of a single oscillator to avoid having to control many different individual physical carriers of quantum information. It encodes discrete quantum information in the continuous space of a quantum system, forcing it to be positioned at regularly spaced points forming a comb with teeth at fixed intervals, effectively digitizing space (see image below). Information is stored in the size of the comb teeth. Small displacements of the comb in position can be corrected, so long as they do not cause neighbouring teeth to overlap. While this scheme was proposed in 2001, an experimental demonstration of error correction with GKP codes came only in 2020, but the degree of error correction that could be achieved was somewhat limited. This is because the GKP code is exact only for quantum states of infinite energy, whereas experiments naturally involve finite- energy states. Brennan de Neeve, a doctoral student in the Home group, Dr Thanh- Long Nguyen, a postdoctoral researcher there, and Tanja Behrle, another doctoral student, have now tackled just that issue.

Coping with finiteness

The team used a platform in which quantum information is encoded in the mechanical oscillator motion of a single trapped ion. This was the same system in which the Home group pioneered the generation and control of logical states of the GKP code. Building on these capabilities, de Neeve et al. now designed and implemented a novel measurement scheme that is optimized for finite- energy states. Their approach is relatively simple to realize, in that it makes use of damping processes which avoid having to measure the quantum state and subsequently apply classically controlled feedback. Putting the new method into practice, they demonstrated efficient correction of unwanted displacements in the motion of their quantum oscillator. As a result, they extended the coherence time (in essence the lifetime of the quantum state) by a factor of three, setting a benchmark for quantum computing systems.

Such prolonged coherence times are important, as they translate directly into more time for executing quantum computations, a key 'currency' when it comes to practical devices. The work therefore addresses one of the grand challenges in the field of quantum computing. Moreover, the new approach uses variants of well- established techniques in the tool chest of experimental quantum physics, inspiring confidence that it can be pushed even further. Combined with progress on other fronts, this brings us ever closer to eventually enabling quantum computers to perform calculations with arbitrary precision, even if constructed from fault- prone components.

18.Rigetti Computing Announces Commercial Availability of 80-Qubit Aspen-M System And Results of Clops Speed Tests

by Lauren Rugani
https://www.globenewswire.com/news-release/2022/02/15/2385386/0/en/Rigetti-Computing-Announces-Commercial-Availability-of-80-Qubit-Aspen-M-System-and-Results-of-CLOPS-Speed-Tests.html?utm_source=ActiveCampaign&utm_medium=email&utm_content=Rigetti+February+2022+Newsletter&utm_campaign=February+2022+Newsletter

Rigetti, a pioneer in hybrid quantum-classical computing, today announced the commercial availability of its 80-qubit quantum system, Aspen-M. The system is available today to the company's direct and distribution customers through Rigetti Quantum Cloud Services (QCS). Rigetti also reported results of system speed tests run on Aspen-M.

"Last year we introduced the world to our proprietary multi-chip technology. We believe our approach to building quantum computers has tremendous advantages, including allowing us to meet the challenges of scaling to systems capable of solving real-world problems," said Rigetti founder and CEO, Chad Rigetti. "Aspen-M is our first commercial system based on this multi-chip technology. Today, we are excited to make Aspen-M generally available to our customers and to release the initial results of system speed tests run on Aspen-M through our production platform."

Aspen-M System Availability

Aspen-M is now available on Rigetti Quantum Cloud Services and will support a number of Rigetti collaborations taking place with both enterprise and public sector customers including Nasdaq, Deloitte, DARPA and the U.S. Department of Energy. Beginning today, Aspen-M will also be available to end users on Amazon Braket, marking the latest in a series of increasingly powerful Rigetti systems offered through the service since Amazon Braket's launch in 2019. In addition, Rigetti expects the 80-qubit system to be available through Azure Quantum, Strangeworks QC™ and Zapata's Orquestra™ platform in the coming months.

Aspen-M's System Speed Tests

Circuit layer operations per second, or CLOPS, characterizes quantum processing speeds inclusive of gate speeds, reprogrammability, and co-processing capabilities, among other factors. Rigetti has customarily tracked gate speed as a key speed metric. CLOPS is designed to characterize how many circuits can run on a quantum computing system in a given unit of time. It leverages the quantum resources on a device to run a collection of circuits as fast as possible, while stressing all parts of the execution pipeline. CLOPS was initially developed and published by IBM in October 2021.

Rigetti reported today its results based on CLOPS for its most recent 40-qubit system, Aspen-11, and for its 80-qubit Aspen-M system. Conducting tests based on 100 shots, as set forth in the original published definition, the 40-qubit Aspen-11 system demonstrated a CLOPS of 844, while the 80-qubit Aspen-M system demonstrated a CLOPS of 892. These results suggest that current Rigetti systems perform as well or better on this CLOPS speed test as the number of qubits in the system increases. By comparison, IBM's published CLOPS scores for systems with 5, 27, and 65 qubits were 1419, 951, and 753, respectively, as of the October 2021 publishing date.

To reflect what users can potentially expect in typical use cases, Rigetti also evaluated CLOPS using 1000 shots. In this case, Aspen-11 performed at 7512 CLOPS and Aspen-M performed at 8333 CLOPS, demonstrating that comparable or better system speed persists at both higher shot counts and higher qubit counts. These speed tests were conducted using the production Rigetti QCS environment.
CLOPS is calculated as $\frac{M \times K \times S \times D}{time\ taken}$, where: $M =$ number of templates = 100; $K =$ number of parameter updates = 10; $S =$ number of shots = 100 (or 1000); and $D =$ number of QV layers $= \log_2 QV$. To Rigetti's knowledge, CLOPS as a speed test has not been investigated or verified by any independent third party. In addition, while Rigetti applied the above formula in testing the speed of Aspen-M and Aspen-11, there is no guarantee that Rigetti applied the test in the same way as IBM and, as a result, any variability in the application of the test as between Rigetti, IBM or others in the industry that may apply CLOPS in the future could render CLOPS scores incomparable and actual relative performance may materially differ from reported results.

Other than IBM, others in the industry have not announced CLOPS as a speed test. As a result, the speed of other competitors as measured by CLOPS is not currently known. In addition, the solution accuracy provided by quantum computers is another key factor, and a quantum computer that may be slower may be preferable to users if it provides a more accurate answer for certain applications. Moreover, the relative leads reflected by speed tests such as CLOPS can change as new generations of quantum computers are introduced by industry participants and, consequently, any advantages cannot be considered permanent and can be expected to change from time to time. Current CLOPS tests may not be indicative of the results of future tests.

19.Warning Over Mysterious Hackers That Have Been Targeting Aerospace And Defence Industries For Years

by Danny Palmer
https://www.zdnet.com/article/these-prolific-hackers-have-been-targeting-the-aerospace-and-defence-industries-with-trojan-malware-for-years/

An unknown criminal hacking group is targeting organisations in the aviation, aerospace, defence, transportation and manufacturing industries with trojan malware, in attacks that researchers say have been going on for years.

Dubbed TA2541 and detailed by cybersecurity researchers at Proofpoint, the persistent cyber-criminal operation has been active since 2017 and has compromised hundreds of organisations across North America, Europe, and the Middle East.

Despite running for years, the attacks have barely evolved, broadly following the same targeting and themes in which attackers remotely control compromised machines, conduct reconnaissance on networks and steal sensitive data.

"What's noteworthy about TA2541 is how little they've changed their approach to cybercrime over the past five years, repeatedly using the same themes, often related to aviation, aerospace, and transportation, to distribute remote access trojans," said Sherrod DeGrippo, vice president of threat research and Detection at Proofpoint.

"This group is a persistent threat to targets throughout the transportation, logistics, and travel industries."

Attacks begin with phishing emails designed to be relevant to individuals and businesses in the sectors being targeted. For example, one lure sent to targets in aviation and aerospace resembles requests for aircraft parts, while another is designed to look like an urgent request for air ambulance flight details. At one point, the attackers introduced COVID-19-themed lures, although these were soon dropped.

While the lures aren't highly customised and follow regular templates, the sheer number of messages sent over the years - hundreds of thousands in total - and their implied urgency will be enough to fool victims into downloading malware. The messages are nearly always in English.

TA2541 initially sent emails containing macro-laden Microsoft Word attachments that downloaded the Remote Access Trojan (RAT) payload, but the group has recently shifted to using Google Drive and Microsoft OneDrive URLs, which lead to an obfuscated Visual Basic Script (VBS) file.

Interacting with these files - the names of which follow similar themes to the initial lures - will leverage PowerShell functions to download malware onto compromised Windows machines.

The cyber criminals have distributed over a dozen different trojan malware payloads since the campaigns began, all of which are available to buy on dark web forums or can be downloaded from open-source repositories.

Currently, the most commonly delivered malware in TA2541 campaigns is AsyncRAT, but other popular payloads include NetWire, WSH RAT and Parallax.

No matter which malware is delivered, it's used to gain remote control of infected machines and steal data, although researchers note that they still don't know what the ultimate goal of the group is, or where they are operating from.

The campaign is still active and it's been warned that the attackers will continue to distribute phishing emails and deliver malware to victims around the world.

20.Quantum Errors Made More Tolerable

by Andreas Trabesinger
https://phys.org/news/2022-02-quantum-errors-tolerable.html

ETH physicists have modified one of the major schemes for quantum error correction and put it into practice, demonstrating that they can substantially prolong the lifetime of quantum states — a crucial ingredient for future large-scale quantum computers.

In modern computing devices, literally billions of transistors work restlessly in almost perfect harmony. The keys to producing near-perfect computation from devices made from imperfect components are the use of digitisation and error correction, with the latter encompassing procedures to detect and rectify inaccuracies as they occur. The challenge of preventing errors from accumulating is one that future quantum computers have to face as well—in fact it forms the main barrier to realizing useful computations. Alas, the tools that have been perfected for classical computers cannot be applied directly to quantum computers, which play by another set of rules, those of quantum mechanics. Ingenious solutions for quantum error correction have been proposed over the past couple of decades, and recently there has been encouraging progress towards implementing such methods in state-of-the-art quantum computers. Writing in Nature Physics, the group of Prof. Jonathan Home at the Institute for Quantum Electronics report such an experimental realization—one that stands out by factoring in important limitations of physically realistic devices and by being relatively easy to implement compared to other proposed error-correction schemes, thus increasing the relevance of the demonstration for practical quantum computation.

Allowing a quantum of error

The way information is processed in quantum computers differs fundamentally from that in their classical counterparts. This opens up unique computational capabilities, but also calls for novel strategies to deal with errors that occur in the process. More specifically, quantum information cannot be perfectly duplicated, and measurements inevitably alter the fragile quantum states. Nevertheless, with some creative rethinking it is possible to devise measurements that can tell us whether the quantum information has been disturbed. As with classical error correction, the key is to harness redundancy.

Among the innovative ideas that have emerged for quantum error correction, the so-called Gottesman-Kitaev-Preskill (GKP) code is a particularly promising one, using flexible control of a single oscillator to avoid having to control many different individual physical carriers of quantum information. It encodes discrete quantum information in the continuous space of a quantum system, forcing it to be positioned at regularly spaced points forming a comb with teeth at fixed intervals, effectively digitizing space (see image below). Information is stored in the size of the comb teeth. Small displacements of the comb in position can be corrected, so long as they do not cause neighboring teeth to overlap. While this scheme was proposed in 2001, an experimental demonstration of error correction with GKP codes came only in 2020, but the degree of error correction that could be achieved was somewhat limited. This is because the GKP code is exact only for quantum states of infinite energy, whereas experiments naturally involve finite-energy states. Brennan de Neeve, a doctoral student in the Home group, Dr. Thanh-Long Nguyen, a postdoctoral researcher there, and Tanja Behrle, another doctoral student, have now tackled just that issue.

Coping with finiteness

The team used a platform in which quantum information is encoded in the mechanical oscillator motion of a single trapped ion. This was the same system in which the Home group pioneered the generation and control of logical states of the GKP code. Building on these capabilities, de Neeve et al. now designed and implemented a novel measurement scheme that is optimized for finite-energy states. Their approach is relatively simple to realize, in that it makes use of damping processes which avoid having to measure the quantum state and subsequently apply classically controlled feedback. Putting the new method into practice, they demonstrated efficient correction of unwanted displacements in the motion of their quantum oscillator. As a result, they extended the coherence time (in essence the lifetime of the quantum state) by a factor of three, setting a benchmark for quantum computing systems.

Such prolonged coherence times are important, as they translate directly into more time for executing quantum computations, a key 'currency' when it comes to practical devices. The work therefore addresses one of the grand challenges in the field of quantum computing. Moreover, the new approach uses variants of well-established techniques in the tool chest of experimental quantum physics, inspiring confidence that it can be pushed even further. Combined with progress on other fronts, this brings us ever closer to eventually enabling quantum computers to perform calculations with arbitrary precision, even if constructed from fault-prone components.

21.Quantum Leap: Has Next-Gen Computing Moved from Hype to Hope?

by Liam Mannix
https://www.smh.com.au/national/quantum-leap-has-next-gen-computing-moved-from-hype-to-hope-20220209-p59ux6.html

Australian scientists believe they have taken a key step towards building a silicon quantum computer – a device that could take quantum computing from hype to mainstream.

Silicon quantum computers marry quantum technology with the same element – silicon – used in existing computer chips, so can hopefully be easily mass-produced. Australia leads the world in the technology, which competes with at least eight other types of quantum computer.

Despite a decade of hype and billions of dollars in investment, quantum computing in general remains a long way off fulfilling its full promise, experts admit. At this stage, there are few uses for such a computer and scientists remain a long way from building a device that could calculate serious equations.

The Australian-led study, recently published on the front cover of leading journal Nature, shows silicon quantum computers can now be operated with better than 99% accuracy.

"This has long been understood as the next big step you needed to take," says Professor Andrea Morello of the University of NSW, who led the work.

Being 99%-plus accurate seems a small achievement for a computer, but it's a big deal in quantum because it is considered the threshold at which you could scale quantum processors into an actual computer, he says.

Sydney Quantum Academy chief executive Professor Peter Turner, who was not involved in the research, says it's "a worthy milestone, for sure."

Classic computers perform calculations using 1s and 0s. Quantum computers use qubits, which are in a quantum state of both 1 and 0 at the same time. If a qubit is disturbed, it turns back to a 0 or 1 – that extreme fragility impairs their accuracy. Worse, unless your computer is at least 99% accurate, as you add more qubits, the computer becomes even more inaccurate.

A second study from the team, published in Advanced Materials in December, shows the quantum chips can be built using "ion implantation", the same technology used to make silicon chips inside computers and smartphones.

"This ensures that our quantum breakthrough is compatible with the broader semiconductor industry," says Professor David Jamieson, who led that work at the University of Melbourne.

A long way to go

Scientists talk of scaling up quantum manufacturing. But current machines are still hand-built. And making one that can do useful things remains a long way off.

IBM's 127-qubit processor holds the title of world's most powerful quantum computer. A useful machine will need "millions, or even billions of qubits", says Professor Jamieson.

Professor Turner says different people give different forecasts on how long that might take. "Some say five years, some say 50. Some holdouts still say it's impossible," he says.

Quantum computers are not comparable to regular computers: they are not designed to play video games or browse the web. Instead, they are useful for extremely specific problems that are difficult or impossible for classic computers to solve - modelling chemistry and cracking widely used encryption, possibly including bitcoin.

Much is made of the ability to crack encryption, but this may just be a step in an arms race: companies are already working to develop quantum-proof encryption.

Quantum scientists argue you can't design programs until you have the hardware.

"There are fewer than we'd like," admits Professor Turner. "But it's not our generation that's going to discover all these quantum algorithms - it's the kids in high school right now."

Thanks to large investments in the early 2000s, Australia once led the world in quantum computing. It is still a key player, but "we are losing our relevance, there is no doubt about that", says Dr Simon Devitt, managing director of the quantum technology consultancy, H-bar.

"Starting in 2014 we started seeing the rest of the world really ramping up their efforts. And Australia is sitting here twiddling its thumbs."

Dr Devitt says several key quantum research centres, including the Centre of Excellence for Quantum Computation and Communication, are due to close within the next three years unless their funding is renewed.

"We have no idea if Canberra is going to go through with a full-fed initiative in quantum, which is what we really need if we're going to continue to be relevant in this space."

22.Two-Dimensional Material Could Store Quantum Information at Room Temperature

by University of Cambridge
https://phys.org/news/2022-02-two-dimensional-material-quantum-room-temperature.html

Researchers have identified a two-dimensional material that could be used to store quantum information at room temperature.

Quantum memory is a major building block to be addressed in the building of a quantum internet, where quantum information is securely stored and sent via photons, or particles of light.

Researchers from the Cavendish Laboratory at the University of Cambridge, in collaboration with colleagues from UT Sydney in Australia, have identified a two-dimensional material, hexagonal boron nitride, that can emit single photons from atomic-scale defects in its structure at room temperature.

The researchers discovered that the light emitted from these isolated defects gives information about a quantum property that can be used to store quantum information, called spin, meaning the material could be useful for quantum applications. Importantly, the quantum spin can be accessed via light and at room temperature.

The finding could eventually support scalable quantum networks built from two-dimensional materials that can operate at room temperature. The results are reported in the journal Nature Communications.

Future communication networks will use single photons to send messages around the world, which will lead to more secure global communication technologies.

Computers and networks built on the principles of quantum mechanics would be both far more powerful and more secure than current technologies. However, in order to make such networks possible, researchers need to develop reliable methods of generating single, indistinguishable photons as carriers of information across quantum networks.

"We can send information from one place to another using photons, but if we're going to build real quantum networks, we need to send information, store it and send it somewhere else," said Dr. Hannah Stern from Cambridge's Cavendish Laboratory, the study's co-first author, along with Qiushi Gu and Dr. John Jarman. "We need materials that can hold onto quantum information for a certain amount of time at room temperature, but most current material platforms we've got are challenging to make and only work well at low temperatures."

23.An Introduction to Post-Quantum Public Key Cryptography

by Joseph Stephen Savariraj
https://www.infoq.com/articles/post-quantum-cryptography-introduction/

Quantum computers are not yet commercially ready and not easy to build, but they promise to outperform today's existing supercomputers. History has proved that technology that seems complex today will reach commercial use in the future, and building quantum computers and using them is surely not feasible now, but that might not always be the case in the future. In fact, many organizations like Google, IBM, Microsoft are doing a lot of research to bring quantum computers into being for practical use.

If quantum computers become ready for commercial application, what will be their use, and what impact will they have? Foreseeably, their use is going to be enormous, and this may benefit many industries and even change our lives. Some of the areas that could benefit are artificial intelligence and machine learning, computational chemistry, drug design, weather predictions, and the list goes on.

Though there are a lot of benefits to be expected from quantum computers, they pose a huge risk for public key cryptography, which is the backbone of all secure connections on the internet today.

In this article, we will discuss the impact quantum computers are predicted to have on public key cryptography based on the topics listed below:

- Quantum computers
- Public key cryptography
- Quantum threat to PKI
- Shor's and Grover's Algorithm
- Post-quantum Cryptography
- Post-quantum Migration

Quantum computers

Though quantum computers are in their initial stage, the research and the speed at which the inventions are taking place can make them operational in a decade or two. Quantum computers can replace supercomputers, which are classical computers with thousands of classical CPU and GPU cores. In 2017 IBM started working with clients on a new generation of electric vehicles with quantum battery technology aimed to reduce atmospheric carbon emissions using quantum computing-aided material discovery.

Quantum computers are systems that use the properties of quantum states to perform computations. In today's computers and PDA devices, the data is represented in bits as 0 or 1, but in quantum computers, 0 and 1 exist simultaneously in different combinations at the same time. The ability to exist simultaneously at the same time is called superposition.

Quantum bits are constituted of a physical system made from the spin of an electron or the orientation of a proton. Electrons, when they spin, behave like tiny magnets, and this orientation always results in 0 pointing up and 1 pointing down. Similarly, a photon behaves like an electromagnetic field with 0 as horizontal polarization and 1 as vertical polarization. These properties of spin and orientation can be found in many different arrangements, forming the basis for quantum computing and linked together with a property known as quantum entanglement.

In the rest of the article, we will see how quantum computers are going to impact public key cryptography which is the backbone of all secure connections.

Public key cryptography

Public key cryptography (PKC) is the basis for today's secure interactions over the Internet. Public key cryptography is asymmetrical, meaning it uses two keys: one is public, which is shared with everyone, and the other is a private key used by the system to prove its identity. The client sends a message to the receiver by generating the hash of the message and encrypting it with the public key. The server uses its key, the private key, to decrypt the message, which can be decrypted only by the corresponding private key and not with any other key, even in case of a middle man attack.

The server proves to the client that it is the intended server and no one else by showing a certificate obtained from the Certificate Authority (CA). The CA follows all required PKI standards and guidelines to issue a certificate to the server and signs it with its private key. The client validates the digitally signed certificate with its trust store, which contains the public keys shared by the CA. Once the certificate has been validated, the client and server establish a symmetric key for the rest of the session because the asymmetric key is slower than the symmetric key.

The keys provided by the CA are used by the algorithm to encrypt and decrypt the plain text. The RSA algorithm, named after its inventors Rivest, Shamir, and Adelman, is the most used among such algorithms.

The keys, both public and private, are prime numbers. In the asymmetric key setup, two prime numbers are taken, p and q, which constitute the private key. Their product $p \times q$ constitutes the public key. It would be easy for small numbers p and q to find its prime factors. If the same number has 200 or 400 digits, though, factoring it into its prime numbers is difficult for any current, classical computer, and it would take millions or trillions of years.

Quantum threat to Public Key Cryptography

The difficulty of factoring prime numbers has allowed public key cryptography to work for many decades without any issues. But with the creation of quantum computers, public key cryptography is at risk because factoring large numbers into primes could take only hours. The NIST predicts that quantum computers will be fully operational in a decade, and they will be able to break asymmetric key cryptography. Once factoring becomes possible, encrypted data that is considered safe today will be easily decrypted. In other words, data that are encrypted and stored now can be decrypted once quantum computers are available.

The algorithm used in quantum computers to factor numbers was proposed by mathematician Peter Shor. We will discuss its impact on PKC in the next section, along with Grover's algorithm.

Shor's and Grover's Algorithms

Peter Shor showed how to factor a number using quantum computers with the effect of reducing the time required from years down to hours. Shor's algorithm can be used to target asymmetric keys, which are the basis for the PKI. If Shor's algorithm ever becomes practical, then any existing keys and data that are stored anywhere need to be re-encrypted.

Shor's algorithm would impact the key exchange to generate the session keys used to encrypt the data. An eavesdropper can record the encrypted session, and later when quantum computers become available, easily decrypt it. An eavesdropper can also forge the digital signatures a client uses to authenticate the server certificate, resulting in data integrity and authentication loss.

Grover's unstructured key search algorithm, on the other hand, could impact symmetric key encryption. Grover's algorithm uses amplitude amplification to search an item in a list. While it would take a classical computer $\frac{N}{2}$ or N steps, Grover's amplification trick only requires $\sqrt{N}$ steps. A quadratic speedup is a time saver to search items from a long list, but the algorithm has to be executed sequentially to achieve its full quadratic speedup.

Since much parallel processing happens in quantum computers, Grover's algorithm cannot be applied as it requires serial processing. If serial processing is taken into consideration, then the impact of Grover's algorithm on symmetric key encryption is less relevant, and using AES 128 will remain secure. In fact, the symmetric key used in AES can be brute-forced using Grover's algorithm, in roughly 2^{64} iterations for a 128-bit symmetric cryptographic key, or in roughly 2^{128} iterations for a 256-bit key. Hence having a symmetric key of double-length will protect from future quantum attacks.

Post Quantum Cryptography

In order to address the challenges posed by quantum algorithms, post-quantum cryptography will aim to make it difficult for quantum computers to break digital signatures.

Several post-quantum cryptography (PQC) solutions have been proposed, like Lattice-based, code-based, multivariate polynomial cryptography, and hash-based signatures. Most PQC algorithms will use a larger key size, for example, AES with keys greater than today's 128-bit keys. If a large key size is required, changes have to be made to various Internet protocols like Transfer Layer Security (TLS) protocol or the Internet Key Exchange. But none of the above proposals have shown to be the perfect solution for quantum threats, as NIST's Report on Post-Quantum Cryptography (NISTIR 81051) concluded.

It is likely we will have different algorithms for different types of applications because of a number of implementation constraints. One such example is the key size: a large key could be suitable for some applications, but not for others. PQC will develop different standards for new applications to be able to defy both traditional and quantum challenges.

While active research is ongoing to find a solution for existing cryptography, another totally different solution has been proposed: Quantum Key Distribution (QKD). In a network, when two parties communicate through a secure channel, it is still possible for an evil person to look at the ciphertext. With QKD, an eavesdropper can be detected before sending any secure information and the communication between two parties can be stopped in the first place. When an eavesdropper interferes, it affects the quantum state and thereby two parties will come to know about the alteration.

Quantum Key Distribution is the process of transferring symmetric keys securely during the execution of PQC algorithms. For classical systems, sharing the secret symmetric keys through an untrusted medium is going to be a challenge in quantum times. QKD attempts to solve it. In fact, different key distribution algorithms exist using public key schemes that are not RSA or ECC, but QKD offers security guarantees rooted in the laws of physics. Furthermore, it will be resilient to quantum attacks. The reason for this is QKD is achieved by encoding the data using quantum states of light, which is impossible to break for an attacker.

In the PQC era, applications should be able to handle more than one cryptographic algorithm to process both quantum and classical ciphers. Using hybrid key mechanisms would enable new applications to safeguard themselves from quantum threats while maintaining the traditional standards. Eventually, organizations need to prepare for new encryption standards.

Post Quantum Migration

The migration from classical cryptography to quantum-safe cryptography has to be done in a staged manner. This includes compiling a list of inventories of applications that will be in use 10 or 20 years from now, as well as preparing migration and execution plans for the implementation of post-quantum cryptography. The organization should consider any new projects in its long-term roadmap with the quantum threat in mind. Migration has to be done with complete knowledge of the assets and evaluating them in view of the quantum threat. In some cases, the organization might depend on 3rd party software which needs to be assessed, and it should be listed as part of the migration plan. In the case of the PKI strategy, for example, the CA does not change, but the implementation will vary.

While preparing the migration plan, a complete assessment has to be done, including deciding whether the application needs to be migrated at all. In fact, some of the systems can be retired or made obsolete during the redesign. Most organizations follow the PKI strategy for their applications, and certificates issued by the CA will need to be re-issued with quantum-safe certificates. The application may need to consider backward compatibility to support hybrid certificates in some cases.

If a PKI is ready to support the new quantum-safe cryptography, the trust certificates and the certificate chain validation must be updated. When the organizations using the PKI are prepared to move to the quantum-safe PKI, the intermediate and root certificates have to be updated in the store. So, the migration plan should consider the CA's migration plan before migrating to quantum-safe PKI. The stored data which are being used in secure communication need to be migrated because they are vulnerable to future quantum attacks. Risk analysis can be performed, and if any in-tangible assets are found, they can be moved to an identified quarantine zone.

The standards are not in place, yet, but the pace of research is growing. The standard will eventually be ready and everyone should be prepared to migrate to it. Once the new standards are put in place, and organizations adhere to the new PKI standards, the users of the certificates and the organizations producing the self-signed certificates should be aware of this change and get ready for the migration. The migration to the new standard involves understanding the existing PKI standards and the quantum-safe standards to come in.

Conclusions

In this article, we provided a short introduction to current PKC architecture and described the impact quantum computers could have on public-key cryptography.

Though quantum computers are in their infancy, their further development could make them commercially available at a reasonable cost, with multifold impact. When that day comes, all public and private keys will be exposed to quantum threats, a massive risk for every organization. Though public key users do not know the internals of how their data is transferred in a secure way, understanding quantum computing growth and the impact it may have on cryptography is key for everyone, irrespective of their role.

Understanding what and how to migrate to the new, yet to come, quantum-safe cryptography standard is vital for everyone, from the CEO to the engineer implementing it. The migration involves budgeting, planning, migrating, developing, implementing, executing, and ensuring a hybrid implementation is in place.

24.Tips to Mitigate Public-Key Cryptography Risk in A Quantum Computing World

by Francis Gaffney
https://www.helpnetsecurity.com/2022/02/10/public-key-cryptography/

Quantum computing is poised to transform the industry over the next decade. With its promise of breakthrough speed and power, it's easy to understand why there is so much hype around this new technology.

But we must also consider the new cybersecurity risks that quantum computing potentially introduces—especially when it comes to encryption. Public-key cryptography is the traditional encryption method used to protect data, transactions, processes, and more. At a high level, it requires a pair of keys – a public key and a private key – which enables communicating parties to encrypt and decrypt data to protect it from unauthorized access. Public-key cryptography uses encryption algorithms that are designed in such a way that decoding them would take so long that they are theoretically unbreakable. This approach has been very effective in the current world of classical computing.

But quantum computers are significantly more powerful than classical ones. As this technology advances over the next decade, quantum computing is expected to expose vulnerabilities in public-key cryptography encryption algorithms within seconds.

The risk: Legitimate or uncertain?

The threat that quantum computing poses to public-key cryptography is not just fearmongering, it's something every organization must take seriously. In fact, it's such a risk that the U.S. Government is taking a proactive approach to mitigate it.

In October 2021, the Department of Homeland Security (DHS), in partnership with the Department of Commerce's National Institute of Standards and Technology, released guidance to help organizations prepare for the transition to post-quantum cryptography. According to DHS, its roadmap will "help organizations protect their data and systems and to reduce risks related to the advancement of quantum computing technology."

Risk mitigation best practices

When it comes to developing a cybersecurity plan to mitigate the security risks associated with quantum computing, the guidance from DHS is certainly a great place to start. Here are some other tips to consider.

Identify where and for what purpose public-key cryptography is being used within your organization, and then mark those systems as "quantum vulnerable."

Here are a few questions to consider throughout this process:

- What is the system protecting – e.g., key stores, passwords, root keys, signing keys, personally identifiable information (PII)?
- What other systems does the one in question communicate with?
- To what extent does the system share information with other entities outside of the organization?
- Does the system support a critical national infrastructure sector?
- How long does the data need to be protected?
- Is the system a high-value asset based on organizational requirements?
  - E.g., is the system essential for business continuity processes? Is it customer-facing? Could it impact organizational operations?
  - In addition to IT systems, make sure to also consider facilities, housekeeping, fire prevention, physical security measures, environment control systems and other business systems and processes.

Develop a cybersecurity playbook to protect identified systems and limit risk.

Cybersecurity playbooks are specific response plans designed to mitigate zero-day vulnerabilities, such as quantum computing-related threats, and document specific response actions in the event of compromise. All playbooks should include detailed instructions regarding:

- Who to contact (e.g., technical teams, senior management, Legal, HR, etc.) in the event of compromise
- How to understand/triage the incident
- How to reduce the impact of the incident
- Steps to retain evidence or data, if required
- How to remediate and recover from the incident, and
- How to perform a post incident review

Designing and developing a cybersecurity playbook is only the first step in the process. Equally as important to documenting a plan is educating and training staff on their specific roles and responsibilities; continuously testing the plan; and putting reporting frameworks in place to ensure ongoing governance.

No time to act like the present

While it's true that quantum computing isn't expected to reach its full potential for a decade or so, it's important that organizations prepare a post-quantum cybersecurity strategy **now** – especially auditing systems to identify "quantum vulnerable" systems / processes as such audits take some time to complete. If quantum computing will provide unprecedented speed and power to computing, then it is likely it will also bring cybersecurity risks and challenges.

To stay one step ahead, organizations should start preparing today. Only then will they be able to leverage the transformative power of quantum computing without impacting their security risk posture.

25.Duke University, IonQ'S New Quantum Computing Gate Could Lead to More Efficient Quantum Algorithms

by Matt Swayne
https://thequantuminsider.com/2022/02/10/duke-university-ionqs-new-quantum-computing-gate-could-lead-to-more-efficient-quantum-algorithms/

The Duke Quantum Center (DQC) at Duke University and IonQ today announced the invention of a new quantum computing operation with the potential to accelerate several key quantum computing techniques and contribute to scaling quantum algorithms. The new quantum gate is a novel way to operate on many connected qubits at once and leverages the multi-qubit communication bus available on IonQ and DQC quantum computers. Full details of the gate technique can be found on the preprint ArXiv.

The new gate family includes the N-qubit Toffoli gate, which flips a select qubit if and only if all the other qubits are in a particular state. Unlike standard two-qubit quantum computing gates, the N-qubit Toffoli gate acts on many qubits at once, leading to more efficient operations. The gate appears naturally in many common quantum algorithms.

IonQ and Duke's discovery may lead to significant efficiency gains in solving fundamental quantum algorithms, such as Grover's search algorithm, variational quantum eigensolvers (VQEs), and arithmetic operations like addition and multiplication. These use cases are ubiquitous across quantum computing applications, and are core to IonQ's work in quantum chemistry, quantum finance, and quantum machine learning. They are also key components of commonly accepted industry benchmarks for quantum computers, which have already shown IonQ's computers to be clear industry leaders.

"This discovery marks another milestone for IonQ as we lead the charge to demonstrate operations that can only be run on a quantum computer," said Dr. Christopher Monroe, Co-Founder and Chief Scientist at IonQ, and the principal investigator at Duke University responsible for the study. "Moreover, no other available quantum computing architectures—not even other ion-based quantum computers—are able to utilize this new family of N-qubit gates. This is because IonQ's quantum computers uniquely feature full connectivity and a wide communication bus that allows all qubits to talk to each other simultaneously."

IonQ anticipates this research, which was conducted at Duke by Dr. Or Katz, Prof. Marko Cetina, and Monroe, to be integrated into IonQ's quantum computing operating system for the general public to use. Once operational, the N-qubit gates will represent yet another way for IonQ's systems to increase their calculation speed while leveraging the unique properties of the company's quantum computing architecture.

This discovery follows a series of announcements around IonQ's research efforts and preparations for scale. In December, IonQ announced that it plans to use barium ions as qubits in its systems, bringing about a wave of advantages it believes will enable advanced quantum computing architectures. Last year, the team also debuted the industry first Reconfigurable Multicore Quantum Architecture and Evaporated Glass Trap technology, both of which are expected to contribute to scaling the number of qubits in IonQ's quantum computers.

26.Race Not Over Between Classical And Quantum Computers

by Katie McCormick
https://physics.aps.org/articles/v15/19

In the race to achieve the coveted "advantage" of a quantum computer, those developing quantum algorithms are pitted against each other and against those working on classical algorithms. With each potential claim of such an advantage—the successful calculation on a quantum computer of something that is infeasible on a classical one—scientists have designed more efficient classical algorithms against which the quantum algorithms must then be compared. Now, by exactly that route, Jacob Bulmer of the University of Bristol, UK, Bryn Bell of Imperial College London, and colleagues **have knocked down a peg** a recent claim of quantum advantage using a method called Gaussian boson sampling. The team behind that **advantage claim** had asserted that a classical computation of Gaussian boson sampling would take 600 million years on the world's fastest supercomputer. But Bulmer, Bell, and colleagues show that their classical algorithm can do it in just 73 days. This result, along with **other recent improvements** to classical algorithms, helps build the case that the quantum-advantage race is far from over.

Gaussian boson sampling is an adaptation of a **2011 idea** from Scott Aaronson of the University of Texas at Austin and Alex Arkhipov, who, at the time, was at the Massachusetts Institute of Technology. The idea, known as boson sampling, proposed sending a beam of single photons through a network of beam splitters to create a complex web of correlations between the paths of the photons.

To imagine the resulting photon-path web, Aaronson and Arkhipov compared their system to a quantum version of a Galton board, a vertical board with pegs fastened to its surface in a two-dimensional pattern. Drop a ball from the top of the board, and it will bounce off the pegs, tracing a random path, until it reaches the ground. If repeated many times, the horizontal distribution of the balls approaches a Gaussian shape. In the case of photons, this distribution should be much more complicated because of the ability of photons to entangle. Aaronson and Arkhipov argued that this distribution likely couldn't be calculated efficiently with a classical computer. The simplicity of the problem made it a good candidate for a near-term demonstration of a quantum advantage.

In 2020, a group of researchers led by Jian-Wei Pan at the University of Science and Technology of China (USTC) did just that using Gaussian boson sampling. This method uses a boson sampler to perform the calculation using squeezed states of light. Photodetectors stationed at the endpoints of all possible paths counted the number of photons that took each path. The team used the sampler to calculate—in 200 seconds—the distribution of the photons through a network of beam splitters with 100 possible paths, something that calculations at the time indicated would take 600 million years on the world's fastest supercomputer, Fugaku. Bulmer, Bell, and their colleagues decide to see if they could reduce that classical calculation time.

Bulmer says that the team knew that one of the main bottlenecks in the classical calculation was determining the "loop Hafnian," a matrix function that is at the heart of simulating Gaussian-boson-sampling experiments. This function gives the probability of measuring a particular distribution of photons at the end of the experiment. The function is inherently difficult to calculate classically, which gives Gaussian boson samplers their advantage over classical computers. Bulmer, Bell, and their colleagues found that they could improve the calculation time by taking advantage of patterns in the structure of the matrix that mathematically describe how photons travel through the maze of beam splitters. This change, along with some other improvements and simplifications, allowed the team to reduce the estimated simulation time of the USTC experiment to just 73 days.

"I think it's great that they've managed to improve the [classical] runtime," Aaronson says. But he adds that the new algorithm developed by Bulmer, Bell, and colleagues "still isn't able to simulate classically, in any reasonable amount of time, the most recent quantum [advantage] experiments" (see **Viewpoint: Quantum Leap for Quantum Primacy**).

While the USTC team's Gaussian-boson-sampling algorithm is still about 4 orders of magnitude faster than that of Bulmer, Bell, and colleagues, some researchers see the factor-of-a-billion drop in classical simulation time as a sign that determining a quantum advantage is a murky problem. "The reality is that this line is not actually well defined," says Alex Moylett, a scientist at Riverlane, UK, a quantum engineering company.

In the distant future, most researchers expect that quantum computers will outperform classical ones by such a large margin that nobody could possibly doubt that they are better. Aaronson has the same hope, but in the meantime, he thinks that classical computers "can, at least for a while, fight back." He says, "developments like these send a message that the experimenters need to up their game if they want [a] quantum [advantage]…to be maintained and improved into the future."

27.Equinix and SK Telecom to Provide Quantum Cryptography Between Data

Centers

by Peter Judge
https://www.datacenterdynamics.com/en/news/equinix-and-sk-telecom-to-provide-quantum-cryptography-between-data-centers/

Equinix is planning to use quantum key distribution (QKD) technology from SK Telecom to secure dedicated lines between its data centers.

The two companies have an agreement to develop QKD, a cryptographic communications technique which quantum entanglement to ensure private distribution of cryptographic keys. The plan is to offer QKD as a service (QaaS) commercially between Equinix data centers. First, the two will test it at an Equinix facility in Seoul, which is believed to be the first data center to use quantum cryptography.

So far, QKD has been mainly applied by telecom companies, and SK Telecom is emerging as a leader in attempts to deliver and commercialize QKD services.

Entangled Web

QKD involves using pair of photons which are entangled quantum mechanically, so whatever happens to one will immediately affect the other. The entangled pair provide evidence that only the intended recipient has accessed a message which includes a cryptographic key, which can then be used in conventional encrypted communications.

SK Telecom is a member of a quantum cryptography project backed by South Korea's government. Through its Geneva-based subsidiary ID Quantique (IDQ), SK Telecom has used QKD to exchange keys for a VPN, thus establishing a "quantum" virtual private network (VPN), which is to say, a regular VPN backed by quantum key exchange. This can then be used over regular shared public networks.

"It will be the first step toward creating synergy between Equinix, a global No. 1 data center operator, and SKT, a global leader in quantum cryptography and 5G wired and wireless communication," SKT's innovation suite head Ha Min-yong said in a statement.

The two plan to make QaaS available in Equinix's data centers and over its interconnections, offering it to protect enterprise-only lines that connect corporate headquarters, offices, and data centers. SKT said the service would become a corporate subscription model in the future.

Equinix sees a possible new business line to address future risks: "As companies gradually adopt digital transformation, cyberattacks are becoming more sophisticated, and digital leaders need a powerful digital infrastructure to address today's threats and take the next step ahead," said Equinix Korea CEO Jang Hye-deok.

In January, the Korean government approved SKT's quantum cryptography transmission encryption modules, so they can in future be used by government organizations and public institutions to protect key information against evolving threats.

28.Germany Expands its Quantum Computing Roadmap With Quast

by Carolyn Mathas
https://quantumcomputingreport.com/germany-expands-its-quantum-computing-roadmap-with-quast/

Germany aims to become a leader in quantum technologies and is rapidly rolling out its roadmap. A newly launched Quantum-enabling Services and Tools for Industrial Applications (QuaST) Consortium will enable rapid quantum adoption without requiring relevant prior knowledge or major investment. QuaST will supply end-users with high-level libraries that automatically decompose a solution into parts requiring classical, high-performance or quantum computing, according to the problem submitted. The parts requiring quantum computing are then optimized and mapped onto the hardware, including a co-design process. Potential applications include logistic optimization, scheduling in production management, health care and drug development and cases from automotive and cybersecurity.

The project is managed by the Fraunhofer Institute for Cognitive Systems IKS, with the additional involvement of such industry partners as the Fraunhofer Institutes for Applied and Integrated Security (AISEC), for Integrated Circuits (IIS), and for Integrated Systems and Device Technology (IISB), the Leibniz Supercomputing Center, and the Technical University of Munich (TUM), as well as companies DATEV eG, Infineon Technologies AG, IQM and ParityQC. The project sponsor is German Aerospace Center (DLR).

Each member brings guidance, technology, training, or funding to the effort. ParityQC, through its architecture and operating system, for example, offers a new approach to optimization encoding and is developing a solution path that automatically finds ideal algorithmic building blocks to solve a problem, and suggesting the most efficient way to encode it on a quantum computer.

The QuaST project emerged from the Munich Quantum Valley initiative for the promotion of Quantum Sciences and Quantum Technologies in Bavaria. QuaST will run until the end of 2024. It has so far received 5.5 million euros ($6.3M USD) in funding, and the total volume of the project amounts to 7.7 million euros ($8.8M USD) with funds provided by Germany's Federal Ministry of Economic Affairs and Climate Action. For more information, access the press release here.

29.Re-Think Security Today For a Post-Quantum World Tomorrow

by Preethi Srinivasan
https://www.dqindia.com/re-think-security-today-for-a-post-quantum-world-tomorrow/

In the near future, quantum computers will be able to perform massive combinatorial computations in a time duration that will outperform the classical computers of today. Quantum computing shifts from today's classical computation fundamentals such as the basic single-state of a bit — 0 or 1. Quantum uses the qubit as the fundamental unit in quantum computing and since the qubit can be in both states at once, it enables faster computations.

As exciting as it is that quantum computing can solve previously unsolvable problems, this power will also enable it to break into your encrypted data or communication.

Post-quantum cryptography

Today, most public key algorithms and digital signatures are not resilient to quantum attacks. The fundamental assumption for today's cryptography and blockchain assets is that it takes enormous computational power and time to breach the system, thus making them safe from almost all cyber threats. For instance, one of the public-key cryptographic algorithms, RSA, that is used in TLS (Transport Layer Security) for secure HTTPS communication, relies on a public encryption key based on the product of two large prime numbers. The prime numbers themselves are kept as the secret to decrypt it. But guess what? Shor's algorithm — a polynomial-time quantum computing algorithm, can perform integer factorization, obtaining back the prime numbers.Thus, a decent quantum computer can rapidly break encryption and digital signature schemes by performing enormous computations quickly.

Post-quantum cryptography (also known as quantum-resistant cryptography) are algorithms that can be secure from attacks caused by a quantum computer. NIST is already evaluating and standardizing quantum-resistant cryptographic algorithms. Some algorithms that have made it to the finals are Classic McEliece, CRYSTALS-Kyber, NTRU, CRYSTALS-Dilithium, FrodoKem, and more.

But, why is post-quantum cryptography important in 2022?

Digital signatures and secure communication like TLS are not resistant to quantum attacks. But why should you care? This style of cryptography is used in applications such as

- Banking
- VPN
- Digital wallets
- Cryptocurrencies such as Bitcoins

It has taken organizations almost 20 years to adopt current cryptographic standards. Robust quantum computing can be expected in the next 10-15 years… you do the math. Unless we start moving now, the vast majority of today's transactions, and user information will be exposed. Many industries will seize the opportunity to get their hands on quantum — from cloud service providers to crypto-currency mining farms. Unfortunately, so will hackers.

So organizations should start preparing now.

Preparing for a post-quantum world

Whether or not you intend to adopt quantum computing for your organization, you will still need to prepare for quantum attacks. A preparation strategy should look something like this:

(i) Educate yourself and your organizational stakeholders about post-quantum cryptography.

(ii) Inspect systems (hardware, software, communication protocols, services, data) and their current encryption methods:

(A) Vulnerable systems which use public key cryptography or digital signatures will need to switch to PQ (Post Quantum) safe algorithms.

(B) Non-vulnerable systems which use symmetric key algorithms or hash functions will need to be inspected if the parameters are PQ safe. For instance, doubling the key sizes of these algorithms can effectively block quantum threats.

(iii) Prioritize areas of focus based on vulnerability, criticality of the system and the expected time and resources required to switch to PQ safe algorithms.

(iv) Set up data retention periods, allowing the organization to begin phasing out old unused data which was encrypted with non-PQ safe algorithms. Leaving this data intact will create vulnerabilities and potential exposure by hackers in a post quantum world.

(v) Look out for NIST standardizations, migration recommendations to post-quantum cryptographic algorithms. It is expected to be finalized between 2022-2024.

(vi) Identify which post-quantum cryptography algorithms and tools will work best for your systems and data.

(vii) Update your cryptographic posture for systems and data for the post-quantum world.

Historically, society has embraced the uses of technology first and then dealt with the adversities caused by it later. For instance, it was exciting when social networks arrived, but the astronomical growth over the last decade has now left us dealing with misinformation. Similarly, with AI and machine learning, it was fascinating to model and build facial recognition models, only later to deal with their biases and the increasing privacy concerns.

But In the case of quantum computing, we are already well aware of the potential threats to come. Now is our opportunity to turn the tide for quantum computing: let's first prepare for quantum threats with post-quantum cryptography so we can enjoy the benefits when quantum computing arrives.

30.Quantum Computing Lab Opens in Lon-

don, Aims to Build World's Largest Quantum Computer

by Matt Swayne
https://thequantuminsider.com/2022/02/08/quantum-computing-lab-opens-in-london-aims-to-build-worlds-largest-quantum-computer/

Quantum Motion, a UK-based quantum computing spinout led by academics from UCL and Oxford University, is leading a wave of technology and science innovation by opening the largest independent quantum computing lab in the UK. The London lab will conduct practical experiments in temperatures 100 times colder than deep space to develop technology to build the world's most powerful computers.

The lab is a multi-million pound investment, backed by funding from the UK government and venture capital and hosts a team of highly specialised scientists and engineers working together to make quantum computing a reality to answer questions that are still impossible for today's computers. It is unique in terms of location, combination of specialist skills and equipment, including several specially configured dilution refrigerators – which cool the quantum chips to near absolute zero (minus 273 degrees Celsius) – making it the most substantial low-temperature facility of any UK quantum company to date.

Based in Islington, north London, the facility will employ 25 full time staff, including quantum theorists, physicists and Integrated Circuit (IC) engineers. This combination of different skills is needed to realise the vision of truly scalable quantum computers based on silicon chips.

"Islington is officially now the coolest part of London," said James Palles-Dimmock, COO of Quantum Motion. "We're working with technology that is colder than deep space and pushing the boundaries of our knowledge to turn quantum theory into reality. Our approach is to take the building blocks of computing – the silicon chip – and demonstrate that it is the most stable, reliable and scalable way of mass manufacturing quantum silicon chips. We've built up a talented team, made major industry breakthroughs and now we're leading the charge of quantum start-up companies in the UK by opening our own independent lab."

A quantum computer harnesses some of the deepest laws of physics, normally seen only at the atomic and subatomic level, giving it unique powers to model the natural world. Quantum computers could be more powerful than today's super computers and capable of performing complex calculations that are otherwise practically impossible, quickly finding new materials, drug discovery or optimising complex processes that can help tackle climate change. The industry has so far managed to create computers with upwards of 100 qubits (quantum bits), but this is orders of magnitude away from the millions of qubits that are needed.

"Quantum bits really change the way a computer is able to think," said Simon Benjamin, co-founder of Quantum Motion and professor of quantum technologies at Oxford University. "Problems that would take a supercomputer thousands of years to crack could be solved by a quantum computer in minutes. Our goal is for quantum computers to be accessible to everyone and that means making it faster and cheaper to manufacture the millions of quantum bits that we need to build into end-devices."

The lab was officially opened by Theo Blackwell MBE, Chief Digital Officer for London on behalf of the Mayor of London. He said, "The Quantum Motion Lab is a great example of world-leading talent, investment and advanced technology coming into London and the UK. Quantum computing represents one of the most exciting emerging technologies we are seeing in our city. In the future, we hope that the power of quantum computing will be able to solve problems faced by people across this city and elsewhere, such as looking for solutions to pollution and air quality, to transport congestion and beyond."

Quantum Motion was founded in 2017 and has raised almost £20m in equity and grant funding, with venture backing from INKEF, IP Group, NSSIF, Octopus Ventures, Oxford Sciences Enterprises and Parkwalk Advisors. The company develops the design and architecture of qubits based on industrial silicon chip manufacturing. Its vision is to use this manufacturing process to produce quantum processors fully integrated with conventional electronics, with high yield and low cost in order to dramatically widen access to quantum computing. In 2021, the Quantum Motion team made a breakthrough discovery that proved quantum computers could be built using standard silicon chips, like those found in any smartphone or computer.

31.The Race to Save The Internet From Quantum Hackers

by Davide Castelvecchi
https://www.nature.com/articles/d41586-022-00339-5

In cybersecurity circles, they call it **Q-day**: the day when quantum computers will break the Internet.

Almost everything we do online is made possible by the quiet, relentless hum of cryptographic algorithms. These are the systems that scramble data to protect our privacy, establish our identity and secure our payments. And they work well: even with the best supercomputers available today, breaking the codes that the online world currently runs on would be an almost hopeless task.

But machines that will exploit the quirks of quantum physics threaten that entire deal. If they reach their full scale, quantum computers would crack current encryption algorithms exponentially faster than even the best non-quantum machines can. "A real quantum computer would be extremely dangerous," says Eric Rescorla, chief technology officer of the Firefox browser team at Mozilla in San Francisco, California.

As in a cheesy time-travel trope, the machines that don't yet exist endanger not only our future communications, but also our current and past ones. Data thieves who eavesdrop on Internet traffic could already be accumulating encrypted data, which they could unlock once quantum computers become available, potentially viewing everything from our medical histories to our old banking records. "Let's say that a quantum computer is deployed in 2024," says Rescorla. "Everything you've done on the Internet before 2024 will be open for discussion."

Even the most bullish proponents of quantum computing say we'll have to wait a while until the machines are powerful enough to crack encryption keys, and many doubt it will happen this decade — if at all.

But the risk is real enough that the Internet is being readied for a makeover, to limit the damage if Q-day happens. That means switching to stronger cryptographic systems, or cryptosystems. Fortunately, decades of research in theoretical computer science has turned up plenty of candidates. These post-quantum algorithms seem impervious to attack: even using mathematical approaches that take quantum computing into account, programmers have not yet found ways to defeat them in a reasonable time.

Which of these algorithms will become standard could depend in large part on a decision soon to be announced by the US National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland.

In 2015, the US National Security Agency (NSA) announced that it considered current cryptosystems vulnerable, and advised US businesses and the government to replace them. The following year, NIST invited computer scientists globally to submit candidate post-quantum algorithms to a process in which the agency would test their quality, with the help of the entire crypto community. It has since winnowed down its list from 65 to 15. In the next couple of months, it will select a few winners, and then publish official versions of those algorithms. Similar organizations in other countries, from France to China, will make their own announcements.

But that will be only the beginning of a long process of updating the world's cryptosystems — a change that will affect every aspect of our lives online, although the hope is that it will be invisible to the average Internet user. Experience shows that it could be a bumpy road: early tests by firms such as Google haven't all run smoothly.

"I think it's something we know how to do; it's just not clear that we'll do it in time," Peter Shor, a mathematician at the Massachusetts Institute of Technology in Cambridge whose work showed the vulnerabilities of present-day encryption, told Nature in 2020.

Even if Q-day never happens, the possibility of code-breaking quantum machines has already changed computer science — and, in particular, the ancient art of cryptography. "Most people I know think in terms of quantum-resistant crypto," says computer scientist Shafi Goldwasser, director of the Simons Institute for the Theory of Computing at the University of California, Berkeley.

.

.

.

32.NTT Scientists Advance Post-Quantum Cryptography at Focs Symposium

by Chris Shaw
https://www.businesswire.com/news/home/20220207005164/en/NTT-Scientists-Advance-Post-Quantum-Cryptography-at-FOCS-Symposium

NTT Research, Inc., a subsidiary of NTT, today announced that two scientists from the NTT Research Cryptography & Information Security (CIS) Lab and NTT Social Informatics Laboratories have written papers selected to be presented at the annual IEEE Symposium on Foundations of Computer Science (FOCS). The FOCS Symposium (FOCS 2021) is taking place virtually, Feb. 7-10, 2022. Event organizers have scheduled 118 presentations over the four-day program. The two papers associated with NTT scientists address aspects of challenges that quantum computing poses to cryptographic systems. One paper, titled "Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier," is co-authored by NTT Research CIS Lab Senior Scientist and Princeton University Assistant Professor Mark Zhandry; the other, "On the Impossibility of Post-Quantum Black-Box Zero-Knowledge in Constant Rounds," is co-authored by Takashi Yamakawa, Researcher, NTT Social Informatics Laboratories. These papers are being presented back-to-back on Feb 7, 2022, Day 1 of the event, at 9:00 am and 9:25 am ET, respectively.

Sponsored by the IEEE Computer Society Technical Committee on Mathematical Foundations of Computing (TCMF), FOCS is a leading conference in the field of theoretical computer science. The call for papers for this event listed quantum computing as one of sixteen areas of interest. Fully realized, quantum computers hold great promise but also pose threats to existing public-key cryptosystems. These NTT-affiliated papers point to areas that are – and are not – likely to be feasible going forward. The "Post-Quantum Succinct Arguments" paper co-authored by Dr. Zhandry introduces a powerful technique to facilitate "rewinding" in the quantum state. The "Post-Quantum Black-Box Zero-Knowledge (ZK)" paper co-authored by Dr. Yamakawa, on the other hand, demonstrates that very efficient ("constant round") ZK proofs may not be possible in the quantum state.

"We were excited to learn that FOCS had selected these two papers, which break new ground in our understanding of post-quantum cryptography and deserve widespread attention," said NTT Research CIS Lab Director Tatsuaki Okamoto. "I also hope that their positions as 'leadoff batters' on Day 1 augur well for the success of this prestigious conference."

In the paper by Zhandry (and Alessandro Chiesa, Fermi Ma and Nicholas Spooner), rewinding is an important tool for security reductions. In cryptography, security is proved by means of a reduction, which transforms an adversary into an efficient algorithm for the hard problem – such as factoring integers or lattice structures – around which a given cryptosystem is designed. In rewinding, the reduction runs the adversary to a certain point in time, backtracks to a previous step, changes the adversary's view in some way, and then runs the adversary again. The program state of a quantum algorithm, however, is very delicate and generally is destroyed when running the adversary. The paper develops a powerful new rewinding technique for quantum adversaries. By combining this technique with Learning With Errors (LWE)-based collapsible hashes, the paper proves the post-quantum security of a thirty-year-old succinct argument system (Kilian's protocol) for which no reduction compatible with quantum attackers was previously known.

The second paper by Yamakawa (and Nai-Hui Chia, Kai-Min Chung and Qipeng Liu) focuses on ZK interactive proofs, fundamental cryptographic primitives that allow one party (the prover) to prove to another party (a malicious verifier) without revealing additional information, except that the statement is true. These protocols have been expressed in a range of languages, including those classified as non-deterministic polynomial (NP) hard. Apart from their wide expression, ZK proofs also exhibit efficiency, even in NP. They achieve constant rounds of communication vs. super-constant rounds, which add significant latency. How they do so is through rewinding (see above) and providing black-box access to the malicious verifier. A post-quantum ZK protocol has been introduced using a technique other than the quantum-averse rewinding, but it requires a super-constant number of rounds and, hence, suffers from latency issues. Non-black-box techniques are also available, yet they can be computationally inefficient as well, incurring slow-downs by factors of 1 million or more. Thus, this paper's negative, though intriguing conclusion: very efficient ZK proofs may not be quantumly possible.

"What I find very interesting about Takashi's work is that it highlights a really subtle issue with quantum algorithms: the nature of time," said Dr. Zhandry, who has sponsored Dr. Yamakawa as a visitor to Princeton. "Algorithms will often have different running times on different inputs, or even variable running times on the same inputs. Classically, this isn't much of an issue; however, quantumly, Takashi's work shows that these variable run times can be quite problematic." About his paper on the rewinding barrier, Dr. Zhandry pointed to the quantum threat of overriding Kilian's protocol, convincing someone of a false statement because prior techniques could not rewind enough: "Our result shows that there is nothing to worry about, provided you use a collapsing hash function inside the protocol."

33.6 Reasons We Need to Start Thinking About Quantum Computing Now

by Deborah Lynn Blumberg
https://www.mastercard.com/news/perspectives/2022/quantum-computing-financial-services/

Quantum computing used to sound like something out of a sci-fi film. The technology uses principles of quantum physics to solve complex problems exponentially faster than today's supercomputers can.

Today, quantum computing is becoming a reality. According to one recent survey, 69% of global enterprises have already adopted or plan to adopt quantum computing in the near term, while the emerging technology is estimated to create up to $850 billion in annual value by 2040.

While classical, or traditional computers, can perform the same tasks as quantum computing, they take much longer — for an especially complex problem, perhaps thousands or even millions of years. Traditional laptops and servers won't go away, says Steve Flinter, head of research and emerging technology at Mastercard Foundry. "We'll see a hybrid, integrated approach where the right device will be used to solve a problem," he says. "Quantum will solve a specialized range of hard and interesting problems."

It's already beginning to transform financial services. Last week, experts across the industry shared insights into the technology, the potential it holds and the risks it could pose at a Mastercard Foundry Live event.

Here are six things you need to know about going quantum:

01 In financial services, the applications are endless — and they're already in the works.

Companies are exploring applications that could help with portfolio optimization, secure communications, transaction settlements and ultrafast trading platforms. Alan Baratz, CEO of quantum computing company D-Wave Systems, has been working with a customer on a fraud detection system that taps into machine learning and a combination of classical and quantum computing, and financial services company BBVA has worked on optimizing portfolios within a given risk profile. With quantum computing, they crunched the data in less than three minutes, as compared with 30 hours with a traditional computer.

02 Quantum computing will help create highly customized experiences for customers.

Today's customers expect high degrees of personalization, and quantum computing can help deliver on that expectation — again through its unique power to analyze huge numbers of potential combinations of options or solutions. "There's clearly a trend toward the idea of 'bank of me,' " Flinter says. "Customers are looking for highly personalized solutions, and I think quantum becomes a part of that solution."

03 Opportunities abound, but so do risks

In the past few years, quantum computing has moved from the research lab into engineering, and it can quickly solve important, complex problems as it simultaneously considers all possible solutions. Though likely years away, bad actors using quantum computing's power may be able to more easily decrypt messages sent using existing public-key cryptography and ultimately compromise the security of key systems that are not quantum-proofed.

04 Quantum computing could help the planet

It's too early to say for sure, but quantum computing applications may well emerge that could help with sustainability, says Robert Sutor, technology leader for quantum computing research at IBM Research. For example, quantum computing could help better predict weather patterns, allowing airlines to more efficiently reschedule and reroute flights when storms hit, ultimately helping them use less fuel.

05 The field is very much still evolving

Expect major advancements over the next five to ten years not just in quantum computing, but also in artificial intelligence and blockchain. “Where these streams will cross will be very interesting,” says Peter Bordow, head of quantum and emerging technology research and development at Wells Fargo. “We may end up in different areas that we haven’t even thought of yet.”

06 Companies should start preparing now

Top of mind should be cybersecurity and the risk that quantum poses to networks and systems. Companies should uncover their vulnerabilities and migrate to more advanced encryption schemes, but, Bordow says, “it’s not as simple as ‘lift and shift,’ or replacing one algorithm for another. There’s a complex landscape of potential solutioning.” Start recruiting the next generation of quantum scientists and developers, too, he advises, form partnerships and think about acquisitions. “Take a metered approach,” he adds. “This is not a sprint, but a marathon.”

34.New Super-Conducting Technology Takes Data Beyond Ones And Zeroes

by Duke University
https://scitechdaily.com/new-super-conducting-technology-takes-data-beyond-ones-and-zeroes/

Leveraging electron spin adds a new dimension to data encoding.

Remember flip-phones? Our smartphones may one day look just as obsolete thanks to spintronics, an incipient field of research promising to revolutionize the way our electronic devices send and receive signals.

In most current technologies, data is encoded as a zero or a one, depending on the number of electrons that reach a capacitor. With spintronics, data is also transferred according to the direction in which these electrons spin.

In a new study appearing this week in the Proceedings of the National Academy of Sciences, a team of Duke University and Weizmann Institute researchers led by Michael Therien, professor of Chemistry at Duke, report a keystone achievement in the field: the development of a conducting system that controls the spin of electrons and transmits a spin current over long distances, without the need for the ultra-cold temperatures required by typical spin-conductors.

“The structures we present here are exciting because they define new strategies to generate large magnitude spin currents at room temperature,” said Chih-Hung Ko, first author of the paper and recent Duke chemistry Ph.D.

Electrons are like spinning tops. Spin-up electrons rotate clockwise, and spin-down electrons rotate counter-clockwise. Electrons with opposite spins can occupy the same volume, but electrons that spin in the same direction repel themselves, like magnets of the same polarity.

By controlling the way that electrons spin along a current, scientists can encode a new layer of information into an electric signal.

Rather than simply turning capacitors on and off in a binary fashion, spintronic devices could also send signals according to the electron's spin, where spin-up may mean something different than spin-down.

"Since the spin can be up or down, that's a piece of binary information that's not harvested in conventional electronic devices," said David Beratan, professor of chemistry and physics at Duke and coauthor of the paper.

Ordinary device currents are composed of equal numbers of spin-up and spin-down electrons. At room temperature, it is challenging to generate a current composed largely of a single spin. The spins flip around, collapse onto one another, drop out of line, and deform the signal like a bad game of telephone.

Now, Therien and his team have developed a strategy to build molecular conductors that keep the electrons in line, ensuring that all of them are spinning in harmony and propagating the direction of spin over long distances, allowing signals to be transmitted with high fidelity, at room temperature.

"It's all about the persistence of that spin polarization," Beratan said. "These spins get jostled around, they interact with the surrounding molecules, with whatever might be nearby, and that can flip them. Here their spin orientation persists, over long times and long distances. They remain in line."

Electrons that spin in the wrong direction can be filtered out of a system using a special class of molecules called chiral molecules.

Chiral molecules are molecules distinguished by having a handedness. Like our right and left hands, these molecules are mirror-images of each other. They can be left-handed or right-handed, and their handedness serves as a filter for electron spins. Just like you'd get ejected from a treadmill if you stopped walking in the right direction, electrons that spin in a direction opposite to the molecule's handedness get filtered out.

Therien and his team had previously developed structures called molecular wires – molecules daisy-chained to one another in a wire-like fashion, that can very easily propagate electric charges. In this new study, the team manipulated these molecular wires and added chiral elements, obtaining a system that not only transmits charge at very low resistance, but transmits charges of the same spin, by forcing all electrons to spin the same way.

"We've integrated for the first time charge propagating and spin polarizing functions in the same molecular wire," Therien said.

Ron Naaman, professor at the Weizmann Institute whose laboratory constructed devices based on Therien's molecules, said that the spin-selective transport enabled by these systems offers tremendous potential for encoding and transmitting information.

The fact that these molecular wires transmit spins at room temperature makes them promising for the development of new technologies.

"To selectively transmit spin at room temperature over long distances without dephasing opens up opportunities for a wider range of devices, and may be important for quantum information science," Therien said.

"Having to cool down your computer with liquid nitrogen wouldn't be very practical," Beratan said. "If we can process spins at room temperature effectively, it would really be a breakthrough in their practical application."

35.Quantum Computing: Researchers Achieve 100 Million Quantum Operations

by Francisco Pires
https://www.tomshardware.com/news/quantum-computing-researchers-achieve-100-million-quantum-operations

Researchers with the U.S. Department of Energy's (DOE) Argonne National Laboratory and the University of Chicago have achieved a new record in maintaining quantum bits (qubits) in a coherent quantum state for more than five seconds. The research, published in the Science Advances Magazine, is hailed as an important new step in extracting useful work from quantum computers - one that should scale quantum computing's performance towards the much-sought-after quantum supremacy moment.

Quantum computing systems are notoriously difficult to maintain in coherent states. The fragile nature of the "ordered chaos" is such that qubit information and qubit connection (entanglement) usually deteriorates in scales much lower than a second. The new research brings quantum computing coherency to human-perceivable scales of time. Using a technique they've termed "single shot readout," the researchers used precise laser pulses to add single electrons to qubits.

"[The] emitted light reflects the absence or presence of the electron, and with almost 10,000 times more signal," said University of Chicago graduate student Elena Glen. "By converting our fragile quantum state into stable electronic charges, we can measure our state much, much more easily. With this signal boost, we can get a reliable answer every time we check what state the qubit is in. This type of measurement is called 'single shot readout,' and with it, we can unlock a lot of useful quantum technologies."

The addition of single electrons is akin to pressing the reset button on your PC, but for quantum states. It eliminates all previously-loaded errors (qubits are sensitive to any external interference), allowing coherent states to "perpetuate" themselves. The idea is to bridge the quantum and electron realms, and the choice of material is paramount: the researchers took advantage of the inherent capabilities of silicon carbide, which can operate in both realms.

"We've essentially made a translator to convert from quantum states to the realm of electrons, which are the language of classical electronics, like what's in your smartphone," said Chris Anderson of the University of Chicago, co-first author on the paper. "We want to create a new generation of devices that are sensitive to single electrons, but that also host quantum states. Silicon carbide can do both, and that's why we think it really shines."

While it may not sound like much, time flows differently in computing; going from stable quantum states in the order of fractions of a second up to five seconds increases the amount of useful computing time extracted from the available qubits. Moreover, it opens up new ways of increasing processing power beyond pure qubit count - the researchers calculate that they can perform around 100 million quantum operations in that five-second slice. So perhaps quantum computing will be a threat to Bitcoin and the current government, commercial and personal encryption schemes much earlier than expected?

"It's uncommon to have quantum information preserved on these human timescales," said David Awschalom, senior scientist at Argonne National Laboratory. "Five seconds is long enough to send a light-speed signal to the moon and back. That's powerful if you're thinking about transmitting information from a qubit to someone via light. That light will still correctly reflect the qubit state even after it has circled the Earth almost 40 times — paving the way to make a distributed quantum internet."

This technology could be paired with photonics-based quantum computing for a scalable, light-speed distributed quantum computing network. The researchers expect their results will allow for the development of quantum repeaters. It is also hoped that through the usage of silicon carbide, there will be venues for typical CMOS (Complementary-symmetry Metal Oxide Semiconductor) manufacturing technologies to integrate electron spin-based systems in classical electrical devices that are sensitive to single charges.

36.Jian-Wei Pan: ‘The Next Quantum Breakthrough Will Happen in Five Years’

by Raúl Limón
https://english.elpais.com/science-tech/2022-02-03/jian-wei-pan-the-next-quantum-breakthrough-will-happen-in-five-years.html

Any leap in quantum computing multiplies the potential of a technology capable of performing calculations and simulations that are beyond the scope of current computers while facilitating the study of phenomena that have been only theoretical to date.

Last year, a group of researchers put forward the idea in the journal Nature that an alternative to quantum theory based on real numbers can be experimentally falsified. The original proposal was a challenge that has been taken up by the leading scientist in the field, Jian-Wei Pan, with the participation of physicist Adán Cabello, from the University of Seville. Their combined research has demonstrated "the indispensable role of complex numbers [square root of minus one, for example] in standard quantum mechanics." The results allow progress to be made in the development of computers that use this technology and, according to Cabello, "to test quantum physics in regions that have previously been inaccessible."

Jian-Wei Pan, 51, a 1987 graduate of the Science and Technology University of China (USTC) and a PhD graduate of Vienna University, leads one of the largest and most successful quantum research teams in the world, and has been described by physics Nobel laureate Frank Wilczek as "**a force of nature.**" Jian-Wei Pan's thesis supervisor at the University of Vienna, physicist Anton Zeilinger, added: "I cannot imagine the emergence of quantum technology without Jian-Wei Pan."

Pan's leadership in the research has been fundamental. "The experiment can be seen as a game between two players: real-valued quantum mechanics versus complex-valued quantum mechanics," he explains. "The game is played on a quantum computer platform with four superconducting circuits. By sending in random measurement bases and measuring the outcome, the game score is obtained which is a mathematical combination of the measurement bases and outcome. The rule of the game is that the real-valued quantum mechanics is ruled out if the game score exceeds 7.66, which is the case in our work."

Covered by the scientific journal Physical Review Letters, the experiment was developed by a team from USTC and the University of Seville to answer a fundamental question: Are complex numbers really necessary for the quantum mechanical description of nature? The results exclude an alternative to standard quantum physics that uses only real numbers.

According to Jian-Wei Pan: "Physicists use mathematics to describe nature. In classical physics, a real number appears complete to describe the physical reality in all classical phenomenon, whereas a complex number is only sometimes employed as a convenient mathematical tool. However, whether the complex number is necessary to represent the theory of quantum mechanics is still an open question. Our results disprove the real-number description of nature and establish the indispensable role of a complex number in quantum mechanics."

"It's not only of interest regarding excluding a specific alternative," Cabello adds, "the importance of the experiment is that it shows how a system of superconducting qubits [those used in quantum computers] allows us to test predictions of quantum physics that are impossible to test with the experiments we have been carrying out until now. This opens up a very interesting range of possibilities, because there are dozens of fascinating predictions that we have never been able to test, since they require firm control over several qubits. Now we will be able to test them."

According to Chao-Yang Lu, of USTC and co-author of the experiment: "The most promising near-term application of quantum computers is the testing of quantum mechanics itself and the study of many-body systems."

Thus, the discovery provides not only a way forward in the development of quantum computers, but also a new way of approaching nature to understand the behavior and interactions of particles at the atomic and subatomic level.

But, like any breakthrough, the opening of a new way forward generates uncertainties. However, Jian-Wei Pan prefers to focus on the positive: "Building a practically useful fault-tolerant quantum computer is one of the great challenges for human beings," he says. "I am more concerned about how and when we will build one. The most formidable challenge for building a large-scale universal quantum computer is the presence of noise and imperfections. We need to use quantum error correction and fault-tolerant operations to overcome the noise and scale up the system. A logical qubit with higher fidelity than a physical qubit will be the next breakthrough in quantum computing and will occur in about five years. In homes, quantum computers would, if realized, be available first through cloud services."

Applications

According to Cabello, "when quantum computers are sufficiently large and have thousands or millions of qubits, they will make it possible to understand complex chemical reactions that will help to design new drugs and better batteries; perform simulations that lead to the development of new materials and calculations that make it possible to optimize artificial intelligence and machine learning algorithms used in logistics, cybersecurity and finance, or to decipher the codes on which the security of current communications is based."

"Quantum computers," he adds, "use the properties of quantum physics to perform calculations. Unlike the computers we use, in which the basic unit of information is the bit [which can take two values], in a quantum computer, the basic unit is the quantum bit, or qubit, which has an infinite number of states."

Cabello goes on to say that "the quantum computers built by companies such as Google, IBM or Rigetti take advantage of the fact that objects the size of a micron and produced using standard semiconductor-manufacturing techniques can behave like qubits."

The goal of having computers with millions of qubits is still a long way off, since most current quantum computers, according to Cabello, "only have a few qubits and not all of them are good enough." However, the results of the Chinese and Spanish team's research make it possible to expand the uses of existing computers and to understand physical phenomena that have puzzled scientists for years.

.

.

.

37.Observation of Quantum Transport at Room Temperature in A 2.8-Nanometer

Cnt Transistor

by National Institute for Materials Science, Japan
https://www.sciencedaily.com/releases/2022/02/220203123008.htm

An international joint research team led by the National Institute for Materials Science (NIMS) has developed an in situ transmission electron microscopy (TEM) technique that can be used to precisely manipulate individual molecular structures. Using this technique, the team succeeded in fabricating carbon nanotube (CNT) intramolecular transistors by locally altering the CNT's helical structure, thereby making a portion of it to undergo a metal-to-semiconductor transition in a controlled manner.

Semiconducting CNTs are promising as the channel material for energy-efficient nanotransistors which may be used to create microprocessors superior in performance to currently available silicon microprocessors. However, controlling the electronic properties of CNTs by precisely manipulating their helical structures has been a major challenge.

This joint research team succeeded for the first time in controllably manipulating CNTs' electronic properties by locally altering their helical structures using heat and mechanical strain. Using this technique, the team was then able to fabricate CNT transistors by converting a portion of a metallic CNT into a semiconductor, where the semiconductor nanochannel was covalently bonded to the metallic CNT source and drain. The CNT transistors, with the channel as short as 2.8 nanometers in length (1 nm = one billionth of a meter), exhibited coherent quantum transport at room temperature -- wave-like electron behavior usually observed only at extremely low temperature.

The molecular structure manipulation technique developed in this research may potentially be used to fabricate innovative nanoscale electronic devices. The team plans to use this technique to engineer material structures with atomic-level precision to fabricate electronic and quantum devices composed of individual atomic structures or molecules.

38.Scientists Estimate That Quantum Computers May Become Powerful Enough to Crack The Bitcoin Encryption in A Decade

by Bogdan Solca
https://www.notebookcheck.net/Scientists-estimate-that-quantum-computers-may-become-powerful-enough-to-crack-the-Bitcoin-encryption-in-a-decade.597437.0.html

Quantum computers are now a thing and many research teams across the world are competing to constantly improve the efficiency and computing power of this new breed of number crunching machines. Back in the mid-2010s, when most researchers were pushing for quantum supremacy over traditional computers, some pointed out that qubits may eventually be used to crack the most sophisticated encryption algorithms in existence, including the SHA-256 one used by cryptocurrencies like Bitcoin. This realization was recently reinforced by Mark Webber and the Ion Quantum Technology team of scientists from the University of Sussex, who calculated what it really takes to break the Bitcoin encryption system and a ballpark estimate of when that could happen.

The SHA (Secure Hash Algorithm) cluster of cryptographic functions was created by the US NSA in the early 2000s. Bitcoin uses the 256-bit version to encrypt all transactions that need to be verified by the mining network before their addition to the blockchain. This is also called proof-of-work consensus because the miners essentially validate how the bitcoin amounts coming from each block are distributed based on the contribution to cracking the cryptographic key assigned to each transaction. The miner or group of miners who succeeds in cracking the key first claims the majority of the bitcoin rewarded per block.

Webber and his team calculated that the fastest quantum computer currently online deployed by IBM with a processing power of 127 qubits is still far from cracking the SHA-256 algorithm in a reasonable time frame. In order to lower the time frame to around 1 hour, the quantum computer would need to harness the power of 317 million qubits, but that will still not be nearly enough to fully crack the code. As Webber puts it, "the transactions get announced and there's a key associated with that transaction. There's a finite window of time when that key is vulnerable and that varies, but it's usually around 10 minutes to an hour, maybe a day." Cracking the code in a 10-minute window actually requires a processor with 1.9 billion qubits.

IBM is confident that it can exponentially increase the qubit number in the next few years, and we could see a processor with millions of qubits in at most 5 years, but reaching billions of qubits may take double that time. There is no immediate threat for the Bitcoin network, yet core developers should consider upgrading the encryption code to make it quantum-resistant by the end of this decade.

39.Quantum Computing Guidelines Issued by World Economic Forum

by Chuck Martin
https://www.iotworldtoday.com/2022/02/02/quantum-computing-guidelines-issued-by-world-economic-forum/

In an attempt to accelerate responsible quantum computing, the World Economic Forum (WEF) has issued a set of guiding principles for the market.

The Quantum Computing Governance Principles provide a framework for stakeholders across different industries and market sectors.

"Assuming that the majority of those involved in developing the technology intend it to have a positive impact on humanity, it is vital to have a set of principles on which key stakeholders such as researchers, developers, users and governments can agree," states the WEF report.

At the center of the principles are seven core values:

- Transparency
- Accessibility
- Non-maleficence
- Equitability
- Inclusiveness
- Accountability
- Common good

The principles were developed with "quantum science and technology experts, business leaders, social scientists, policy-makers and authorities on emerging technology ethics and law" globally.

The principles are organized into nine themes, as stated by the World Economic Forum:

- Transformative capabilities: Harness the transformative capabilities of this technology and the applications for the good of humanity while managing the risks appropriately.

- Access to hardware infrastructure: Ensure wide access to quantum computing hardware.

- Open innovation: Encourage collaboration and a precompetitive environment, enabling faster development of the technology and the realization of its applications.

- Creating awareness: Ensure the general population and quantum computing stakeholders are aware, engaged and sufficiently informed to enable ongoing responsible dialogue and communication; stakeholders with oversight and authority should be able to make informed decisions about quantum computing in their respective domains.

  - Workforce development and capability building: Build and sustain a quantum ready workforce.

  - Cybersecurity: Ensure the transition to a quantum-secure digital world.

  - Privacy: Mitigate potential data-privacy violations through theft and processing by quantum computers.

  - Standardization: Promote standards and road-mapping mechanisms to accelerate the development of the technology.

  - Sustainability: Develop a sustainable future with and for quantum computing technology

The next step is for the governance workstream of the World Economic Forum's Quantum Computing Network to work with stakeholders to adopt the principles.

40.Meet The NSA Spies Shaping The Future

by Patrick Howell O'Neill
https://www.technologyreview.com/2022/02/01/1044561/meet-the-nsa-spies-shaping-the-future/

For someone with a deeply scientific job, Gil Herrera has a nearly mystical mandate: Look into the future and then shape it, at the level of strange quantum physics and inextricable math theorems, to the advantage of the United States.

Herrera is the newly minted leader of the National Security Agency's Research Directorate. The directorate, like the rest of the NSA, has a dual mission: secure American systems and spy on the rest of the world. The budget is classified, a secret among secrets, but the NSA is one of the world's largest spy agencies by any measure and Herrera's directorate is the entire US intelligence community's biggest in-house research and development arm. The directorate must come up with solutions to problems that are not yet real, in a world that doesn't yet exist.

In his first interview since getting the job, Herrera lays out the tech—and threats—his group will now be focusing on. His priorities show how much the NSA's targets are changing, balancing its work surveilling terror groups with an appreciation of how rapidly the geopolitical landscape has shifted in recent years. And he explains why the rise of new technologies, in terms of both threat and opportunity, are at the heart of what his group must contend with.

Herrera takes the helm as the agency faces new challenges. The bipolar world of the Cold War belongs to the history books. The United States' quick turn as a lone superpower is over. The new world is a messier one, defined by an emerging era of great power competition among nations like the United States, China, and Russia. Meanwhile, the NSA is still recovering from a massive set of leaks published nine years ago about global and domestic surveillance programs that set off a firestorm of criticism and calls for reform and changed the average American's perception of the NSA. The companies that worked with them recoiled in embarrassment and anger. And it also changed the way the NSA operates.

"We're at a point now where we need to start focusing more on larger adversaries, more sophisticated adversaries, adversaries that don't necessarily utilize commercial services," says Herrera. "These are adversaries that have their own indigenous services and that create their own technology. So as a research directorate, we need to respond. We need to provide the technologies that allow us to interrogate the huge amounts of information brought to us and to help monitor the kinds of systems that are now emerging as a result of great power competition."

The rate of technological change is accelerating and becoming less predictable.

"Any time there's that kind of a shift, it's complex," says Herrera. "Each generation of technology presents its new challenges."

For example, the directorate has devoted significant resources toward mastering quantum computing, technology that has the potential to break the encryption used to protect sensitive data in the digital world of today and tomorrow. Powerful countries, companies, and universities are pouring money into the task of building a quantum computer powerful enough to perform exponentially faster than the computers of today.

"Great power competition drives the agenda," says Herrera. "It changes the kind of technology and access we need. Technologies like quantum and 5G are part of that."

The directorate has been at the forefront of quantum computing research since 1995, immediately following the advent of Shor's algorithm, which showed how quantum computers can factor numbers exponentially faster than normal computers—exactly the kind of work needed to break encryption.

The directorate's fingerprints now show up in the form of fundamental research advancing the field and even inside the most advanced computers built at giant tech firms. The highly publicized race to build the world's best quantum computer is proof of this: both Google and IBM use the same basic building block in their machines to create quantum behavior, known as transmon qubits, which was invented under the directorate's sponsorship. Historically, the NSA has been the single largest funder of academic quantum computing research, says Herrera.

Herrera is hesitant to discuss specifics about what his directorate is zeroing in on, but when asked about the challenges of spying in a world of rapid technical advancement, he agrees and points to the emergence of 5G around the world. 5G brings its own new challenges for collecting intelligence, Herrera explains. Monitoring 5G successfully requires a deep understanding of what makes it fundamentally different from its predecessors: higher speed, lower range, more distribution nodes, different data protocols.

Understanding what will happen in the world tomorrow requires a mastery of the elements that will define it.

Future history

The NSA's Research Directorate is descended from the Black Chamber, the first group of civilian codebreakers in the United States who were tasked with spying on cutting-edge technology, like the telegraph. Existing only from 1919 to 1929, the group decoded over 10,000 messages from a dozen nations, according to James Bamford's 2001 book Body of Secrets: Anatomy of the Ultra-Secret National Security Agency. In addition to groundbreaking cryptanalytic work, the group succeeded by securing surveillance help from American cable companies like Western Union that could supply the newly minted US spies with sensitive communications to examine.

The Black Chamber was shut down amid scandal when US Secretary of State Henry Stimson found out the group was spying on American allies as well as foes. The incident foreshadowed the 1975 Church Committee, which investigated surveillance abuses by American intelligence agencies, and the 2013 Snowden leaks, which exposed vast electronic surveillance capabilities that triggered a global reckoning.

Just eight months after the Black Chamber was shuttered, the US, faced with the prospect of crippled spying capabilities in the increasingly unstable world of the 1930s, reformed the effort under the Army's Signals Intelligence Service. One of just three people working with the Black Chamber's old records, one of the founders of the SIS, which Bamford reports was kept a secret from the State Department, was the mathematician Solomon Kullback.

Kullback was instrumental in breaking both Japanese and German codes before and during World War II, and he later directed the research and development arm of the newly formed National Security Agency. Within a year, that evolved into the directorate as we know it today: a distinct space for research that is not disrupted by the daily work of the agency.

"It's important to have a research organization, even in a mission-driven organization, to be thinking beyond a crisis," says Herrera, though he adds that the directorate does dedicate some of its work to the "crisis of the day." It runs a program called "scientists on call," which allows NSA mission analysts facing technical challenges while interrogating information to ask for help via email, giving them access to hundreds of scientists.

Forward looking

But the lion's share of the directorate's work is envisioning the technologies that are generations ahead of what we have today. It operates almost like a small, elite technical college, organized around five academic departments—math, physics, cyber, computer science, and electrical engineering—each staffed with 100 to 200 people.

The cybersecurity department defends the federal government's national security and the country's military-industrial base. This is the highest-profile department, and deliberately so. Over the last five years, the previously shadowy NSA has become more vocal and active in cybersecurity. It has launched public advisories and research projects that would once have been anathema for an organization whose existence wasn't even acknowledged until 20 years after its founding.

Now the products of NSA research, like Ghidra, a free, sophisticated reverse engineering tool that helps in the technical dissection of hacking tools, as well as other software, are popular, trusted, and in use around the world. They serve as powerful cybersecurity tools, a recruiting pitch, and a public relations play all wrapped into one.

The physics department, which Herrera once directed, runs dozens of laboratories that conduct most of the work on quantum information sciences, but it has a much wider remit than that. As advancements in raw computing power threaten to slow and halt 60 years of predictably rapid computing growth, its physicists are exploring new materials and novel computing architectures to drive the next generation of computing into a less predictable future, exactly the kind of task the directorate was given when it first came into existence.

Meanwhile, the electrical engineering department has been looking closely at the physics and engineering of telecommunications networks since the internet first arose. As well as the issues around

5G, it also tackles every facet of the digital world, from undersea cables to satellite communications.

Some prospects on the horizon don't fit neatly into any particular box. The computer science department's work on artificial intelligence and machine learning, for example, cuts across cybersecurity missions and data analysis work with the mathematicians.

Herrera repeatedly raises the prospect of the directorate needing to develop greater capabilities in and understanding of rapidly advancing fields like synthetic biology. The NSA is hardly alone in this: Chinese military leaders have called biotech a priority for national defense.

"Much of the competition in the world now is not military," Herrera says. "Military competition is accelerating, but there is also dissemination of other technologies, like synthetic biologies, that are frankly alarming. The role of research is to help the NSA understand what the impact of those technologies will be. How much we actually get involved, I don't know, but these are areas we have to keep an eye on."

Finally, the math department, the directorate's oldest, is unique. Herrera describes math as a core defining work of the directorate. The NSA is the country's biggest employer of mathematicians, and the directorate boasts some of the best. Virtually every other department in the NSA's Research Directorate suffers from having to compete with tech companies and the high salaries available in the private sector. The math department does not have that issue, Herrera says. Silicon Valley typically values software developers more than it does mathematicians.

The math department, often in conjunction with the computer science department, helps tackle one of NSA's most interesting problems: big data. Despite public reckoning over mass surveillance, NSA famously faces the challenge of collecting such extreme quantities of data that, on top of legal and ethical problems, it can be nearly impossible to sift through all of it to find everything of value. NSA views the kind of "vast access and collection" that it talks about internally as both an achievement and its own set of problems. The field of data science aims to solve them.

"Everyone thinks their data is the messiest in the world, and mine maybe is because it's taken from people who don't want us to have it, frankly," said Herrera's immediate predecessor at the NSA, the computer scientist Deborah Frincke, during a 2017 talk at Stanford. "The adversary does not speak clearly in English with nice statements into a mic and, if we can't understand it, send us a clearer statement."

Making sense of vast stores of unclear, often stolen data in hundreds of languages and even more technical formats remains one of the directorate's enduring tasks.

In the digital age, one of the primary goals of spying would be the ability to decode important data are currently protected by strong encryption. That's why the Research Directorate's mathematicians and computer scientists design and break cryptography algorithms for some of the world's most sensitive systems.

The building and breaking of code is at the core of what the directorate does because, when the NSA looks into the future, what it sees is an increasingly digital world filled with data. Its ability to both protect and surveil it will help define great power competition for a long time.

"In the future, superpowers will be made or broken based on the strength of their cryptanalytic programs," a 2007 document from the agency explained. "It is the price of admission for the US to maintain unrestricted access to and use of cyberspace."

"The Research Directorate exists to enable the mission," Herrera says. "From atoms to systems, we do research with the mission in mind."

41.The Power of Chaos: A Robust And Low-Cost Cryptosystem For The Post-Quantum Era

by Ritsumeikan University
https://www.sciencedaily.com/releases/2022/02/220201115235.htm

Fast algorithms on quantum computers could easily break many widely used cryptosystems, necessitating more innovative solutions for digital security. In a recent study, a team of scientists designed a stream cipher consisting of three cryptographic primitives based on independent mathematical models of chaos. The resulting cryptographic approach is robust to attacks from large-scale quantum computers and can be implemented on low-cost computers, paving the way to secure digital communications in the post-quantum era.

While for most of us cryptographic systems are things that just run "under the hood," they are an essential element in the world of digital communications. However, the upcoming rise of quantum computers could shake the field of cryptography to its core. Fast algorithms running on these machines could break some of the most widely used cryptosystems, rendering them vulnerable. Well aware of this looming threat, cryptography researchers worldwide are working on novel encryption methods that can withstand attacks from quantum computers.

Chaos theory is actively being studied as a basis for post-quantum era cryptosystems. In mathematics, chaos is a property of certain dynamic systems that makes them extremely sensitive to initial conditions. While technically deterministic (non-random), these systems evolve in such complex ways that predicting their long-term state with incomplete information is practically impossible, since even small rounding errors in the initial conditions yield diverging results. This unique characteristic of chaotic systems can be leveraged to produce highly secure cryptographic systems, as a team of researchers from Ritsumeikan University, Japan, showed in a recent study published in IEEE Transactions on Circuits and Systems I.

Led by Professor Takaya Miyano, the team developed an unprecedented stream cipher consisting of three cryptographic primitives based on independent mathematical models of chaos. The first primitive is a pseudorandom number generator based on the augmented Lorenz (AL) map. The pseudorandom numbers produced using this approach are used to create key streams for encrypting/decrypting messages, which take the stage in the second and perhaps most remarkable primitive -- an innovative method for secret-key exchange.

This novel strategy for exchanging secret keys specifying the AL map is based on the synchronization of two chaotic Lorenz oscillators, which can be independently and randomly initialized by the two communicating users, without either of them knowing the state of the other's oscillator. To conceal the internal states of these oscillators, the communicating users (the sender and the receiver) mask the value of one of the variables of their oscillator by multiplying it with a locally generated random number. The masked value of the sender is then sent to receiver and vice-versa. After a short time, when these back-and-forth exchanges cause both oscillators to sync up almost perfectly to the same state in spite of the randomization of the variables, the users can mask and exchange secret keys and then locally unmask them with simple calculations.

Finally, the third primitive is a hash function based on the logistic map (a chaotic equation of motion), which allows the sender to send a hash value and, in turn, allows the receiver to ensure that the received secret key is correct, i.e., the chaotic oscillators were synchronized properly.

The researchers showed that a stream cipher assembled using these three primitives is extremely secure and resistant to statistical attacks and eavesdropping since it is mathematically impossible to synchronize their own oscillator to either the sender's or the receiver's ones. This is an unprecedented achievement, as Prof. Miyano states: "Most chaos-based cryptosystems can be broken by attacks using classical computers within a practically short time. In contrast, our methods, especially the one for secret-key exchange, appear to be robust against such attacks and, more importantly, even hard to break using quantum computers."

In addition to its security, the proposed key exchange method is applicable to existing block ciphers, such as the widely used Advanced Encryption Standard (AES). Moreover, the researchers could implement their chaos-based stream cipher on the Raspberry Pi 4, a small-scale computer, using Python 3.8. They even used it to securely transmit a famous painting by Johannes Vermeer between Kusatsu and Sendai, two places in Japan 600 km apart. "The implementation and running costs of our cryptosystem are remarkably low compared with those of quantum cryptography," highlights Prof. Miyano, "Our work thus provides a cryptographic approach that guarantees the privacy of daily communications between people all over the world in the post-quantum era."

With such power of chaos-based cryptography, we may not have much to worry about the dark sides of quantum computing.

42.Efficient Quantum Programming Using Ease Gates on A Trapped-Ion Quantum Computer

by Karine
https://thequantumhubs.com/efficient-quantum-programming-using-ease-gates-on-a-trapped-ion-quantum-computer/

Parallel operations in conventional computing have proven to be an essential tool for efficient and practical computation, and the story is not different for quantum computing. Indeed, there exists a large body of works that study advantages of parallel implementations of quantum gates for efficient quantum circuit implementations. Here, the authors focus on the recently invented efficient, arbitrary, simultaneously entangling (EASE) gates, available on a trapped-ion quantum computer. Leveraging its flexibility in selecting arbitrary pairs of qubits to be coupled with any degrees of entanglement, all in parallel, they show an n-qubit Clifford circuit can be implemented using $6 \log n$ EASE gates, an n-qubit multiply-controlled NOT gate can be implemented using $\frac{3n}{2}$ EASE gates, and an n-qubit permutation can be implemented using six EASE gates. They discuss their implications to near-term quantum chemistry simulations and the state of the art pattern matching algorithm. Given Clifford + multiply-controlled NOT gates form a universal gate set for quantum computing, their results imply efficient quantum computation by EASE gates, in general.