Crypto News

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

July 01, 2023

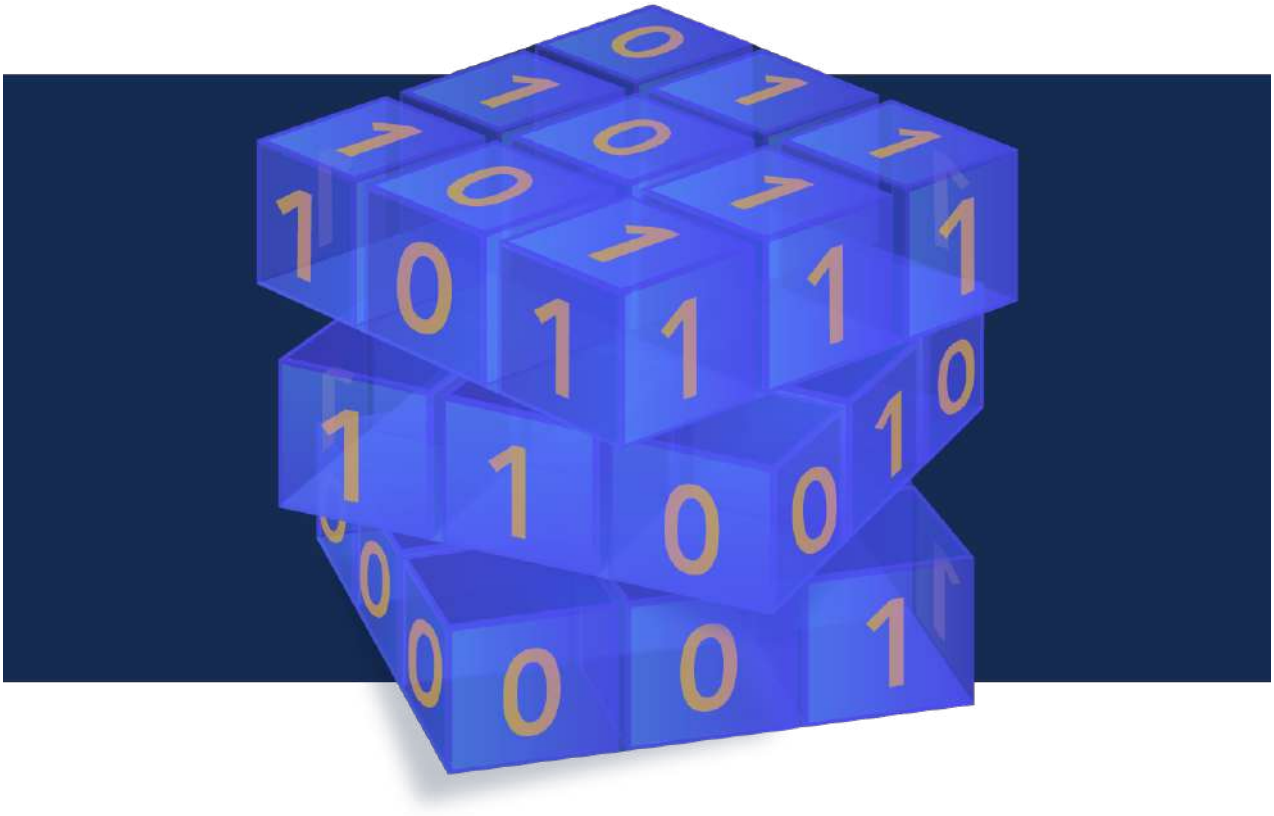


TABLE OF CONTENTS

Editorial

Happy July readers! Let's start with the "Cryptography Arms Race". History buffs know that cryptography has been around for centuries and is something that has evolved with time and is widely used to protect our digital data today. It allows privacy for the general public from hackers and even governments. Those of us working in cybersecurity know that at times, cybersecurity comes at the cost of privacy. This can often create a rift between cybersecurity and privacy professionals. Both sides have valid claims for their areas of expertise and one can see the logic of both is sound. The author of article 19 highlights the importance of privacy and reminds technology professionals to remember its importance for the proper functioning of society. Those of us working in the field of quantum computing are acutely aware of the implications of quantum computers as they relate to privacy, however, the reminder for the general technology community is valid. If this discussion piqued your interest in post-quantum cryptography and data security using quantum computers, head over to articles 25 and 26 to learn more about our options for a post-quantum world.

Next, let's talk about something we haven't touched on for a while, the need for an ever-increasing population of properly skilled technology professionals. For years, the quantum computing community has strongly stated the need to up-skill our current technology professionals as well as ingrain science and technology education for coming generations into our educational systems to ensure that we have the right skill sets for the future. Moving along that line of thinking, the author of article 4 outlines the importance for IT project managers to know how cryptography works. Understanding cryptography for all technology workers is important and making sure to expand the need to IT project managers acknowledges the need for the technology ecosystem to be adequately educated and trained in the relevant topics for our future success. Do you think we're making enough headway when it comes to the number of sufficiently skilled technology professionals or are we falling short? As always, happy reading!

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

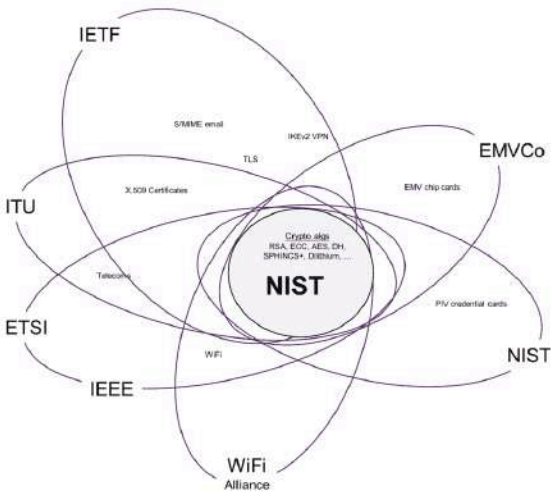
Disclaimer. The QSS WG does not express an opinion on the validity of the ideas and the claims presented in the articles in this newsletter.

1.Post-Quantum Cryptography Advances… Under The Hood

by Iain Beveridge
https://www.entrust.com/blog/2023/06/post-quantum-cryptography-advancesunder-the-hood/

A typical scene at a car enthusiasts motorhead event involves souped-up cars with their hoods propped open and a bunch of grease monkeys gathered around staring at the powerful V12 combustion engine. With the migration to electric cars it is probably a scene that will start to phase out over time. A bit like classical asymmetric cryptography!

There has been a lot of coverage on the anticipated advance of quantum computers: the boon they will bring to medicine, science, and chemistry; and the curse on IT security, with Shor's algorithm sounding the death knell for traditional classic asymmetric cryptography, which underpins the security for most of what we do on the internet. For this blog post I decided to focus on some of the post-quantum cryptography (PQC) related activities that are going on as we speak, under-the-hood. I'm talking specifically about the Internet Engineering Task Force (IETF), who are tasked with preparing the public internet for a post-quantum world, figuring out how to retool and migrate the protocols and standards built on classical algorithms that we rely on extensively today.

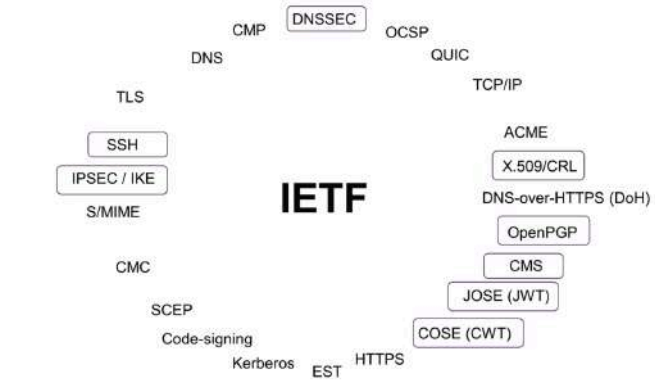


NIST forms the nucleus of the PQC migration, surrounded by a shell of other standards bodies

First to provide a bit of context, it is worth reviewing where the IETF fits in to the PQC story. At the nucleus of figure 1 is National Institute of Standards and Technology (NIST). Their ongoing competition tasked with identifying and standardizing on the PQC primitives has been well-documented. You might already be au fait with some of the short-listed PQC algorithms including SPHINCS+, CRYSTALS-Dilithium and CRYSTALS-Kyber, as well as XMSS and LMS, which are already NIST standards [SP 800-208]. The output of the NIST's work will then be used by a shell of orbiting standards bodies such as the European Telecommunications Standards Institute (ETSI), Institute of Electrical and Electronic Engineers (IEEE), EMVCo, International Telecommunication Union (ITU), and the Wi-Fi Alliance®.

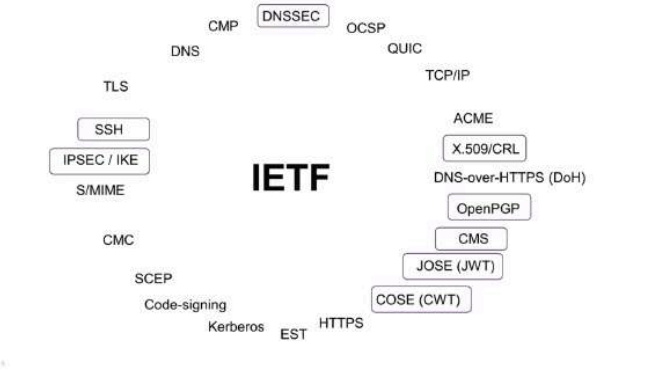
Outside of the NIST's area of responsibility, updating the protocols and technologies that rely on cryptography deemed vulnerable to quantum attacks falls to each of the respective standards bodies to make them ready for a post-quantum world.

Consider the IETF, who own the specifications for many of the internet's cryptographic and security protocols:



Some of the security protocols and standards maintained by the IETF

You might not recognize all of these protocols, but you should be at least vaguely familiar with TLS, SSH, HTTPS, TCP/IP, and DNSSEC, fundamental building blocks for internet communication and security. Fortunately, there is an opportunity to reuse and recycle. The protocols highlighted below are those that need to be retooled with PQC algorithms. The remaining protocols actually don't need updating. They get their cryptography for free by embedding another PQ-safe protocol. So the list is perhaps less daunting than it first appears but still some non-trivial work lies ahead.



IETF security protocols and standards with those requiring PQC retooling highlighted

A couple of my Entrust colleagues, Mike Ounsworth and John Gray, are fully embedded in the IETF Working Groups. They have been working for the past 5 years on defining the standards for composite digital certificates, utilizing a combination of classical and PQ cryptography. Last time I counted they have authored or co-authored 13 papers that will eventually define and specify how communication protocols operate in a post-quantum world – pretty cool stuff! They reported back from their recent IETF

116 session in Tokyo/Yokohama, Japan, where the general MO is “Hurry up and wait.” In essence it means get drafts of these protocols started, then put them in a holding pattern until final NIST specs for CRYSTALS-Dilithium, FALCON, SPHINCS+, and CRYSTALS-KYBER are standardized. As I chatted with my colleagues, one of the things that was clear is their appreciation for just how well-crafted and versatile the classical algorithms and APIs were. I’m referring to those which came from the pioneers of modern-day cryptography such as public key cryptography defined in the ’70s by Rivest, Shamir, and Adleman (RSA), Diffie, Hellman, and Merkle, and others. I imagine it is the equivalent of modern-day car designers gazing under the hood of a vintage E-Type Jaguar or Ferrari in appreciation of its design, power, and finesse. We’re talking about the nuts and bolts of cryptographic algorithms and APIs here: key transport, key agreement, key encapsulation mechanisms (KEMs), double ratchets, and 0.5 (round-time trips) RTTs! What the IETF working groups are finding is that some of the classic algorithm and mechanism properties are very hard to retain when migrating to PQC equivalents. It is proving challenging even for some of the sharpest minds in the industry. However, in a slow and steady pace they are making good progress.

One of the initiatives I learned about from Entrust’s participation in IETF 116 was our support for the new IETF PQUIP (Post-Quantum Use In Protocols) working group. The name PQUIP, a post-quantum spin on the word “equip” was actually coined by my colleague Mike Ounsworth. The PQUIP group was founded in Jan 2023 and recently had its first meeting at IETF 116. The PQUIP charter is here: https://datatracker.ietf.org/wg/pquip/about/ I know my Entrust colleagues are super proud to be founding and active members of this group focused on bringing the entire internet community together to share knowledge and best practices for how to integrate the new PQC algorithms into the myriad IT security protocols that we rely on every day. This is about mathematicians, subject matter experts, software engineers, and cryptographers coming together across academia and industry to pave the way for a smooth transition to PQ. Architecting the largest cryptographic migration that humanity has ever done is no small feat! It involves juggling security against ease-of-deployment for IT admins through often politics-ridden public discussion groups while under a tight and unforgiving deadline!

So far, the primary output of PQUIP is this document cataloging all of the PQC efforts across the IETF. Check out https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc to see how much design work is involved. Also note the listing at the bottom “Security Area protocols with no PQC-specific action needed” referring to the protocols that will get PQC for free.

Eminent mathematician and PQC academic Michele Mosca when asked for his advice to enterprises on preparing for PQ said “make this about lifecycle management not crisis management.” I think it is fair to say that the IETF working groups are implementing those wise words, figuring out the tricky low-level stuff while we have time. I look forward to seeing the output of their good work in the coming months and years.

2.A New Era Of Encryption: The Rise Of Post-Quantum Cryptographic Algorithms

https://citylife.capetown/uncategorized/a-new-era-of-encryption-the-rise-of-post-quantum-cryptographic-algorithms/225171/

A new era of encryption is dawning, and it promises to revolutionize the way we secure our digital lives. With the advent of quantum computing, traditional cryptographic algorithms that have safeguarded our data for decades are now under threat. As a result, researchers and industry experts are scrambling to develop post-quantum cryptographic algorithms to ensure the continued safety of our digital assets and

communications in a quantum world.

Quantum Computers, Unlike Classical Computers, Harness The Power Of Quantum Mechanics To Perform Complex Calculations At Speeds Previously Thought Impossible. While This Breakthrough In Computing Technology Holds Great Promise For Various Fields Such As Medicine, Artificial Intelligence, And Finance, It Also Poses A Significant Risk To The World Of Cryptography. The Encryption Algorithms That Form The Backbone Of Modern Data Security, Such As Rsa And Elliptic Curve Cryptography, Rely On The Difficulty Of Solving Certain Mathematical Problems That Are Infeasible For Classical Computers To Crack. However, Quantum Computers Have The Potential To Solve These Problems Exponentially Faster, Rendering These Cryptographic Methods Obsolete And Leaving Our Digital Lives Exposed.

In Response To This Looming Threat, Researchers Have Been Working Tirelessly To Develop New Cryptographic Algorithms That Can Withstand The Power Of Quantum Computers. This Emerging Field, Known As Post-Quantum Cryptography, Aims To Create Encryption Methods That Are Resistant To Both Classical And Quantum Attacks. Several Promising Candidates Have Emerged, Including Lattice-Based Cryptography, Code-Based Cryptography, And Multivariate Cryptography, Among Others. These Novel Approaches Rely On Mathematical Problems That Are Believed To Be Resistant To Quantum Attacks, Ensuring The Security Of Encrypted Data Even In The Face Of Quantum Computing Advancements.

The Race To Develop Post-Quantum Cryptographic Algorithms Has Gained Significant Momentum In Recent Years, With Organizations Such As The National Institute Of Standards And Technology (Nist) Leading The Charge. In 2016, Nist Initiated A Global Competition To Identify And Standardize Post-Quantum Cryptographic Algorithms. The Competition Has Since Narrowed Down The Field To A Handful Of Promising Candidates, With The Final Selection Expected To Take Place In The Coming Years. Once Standardized, These Algorithms Will Form The Foundation Of A New Era Of Encryption, Providing Robust Security In A Quantum World.

However, The Transition To Post-Quantum Cryptography Is Not Without Its Challenges. One Of The Primary Concerns Is The Need For Widespread Adoption Of These New Algorithms Across Various Industries And Applications. This Process Will Require Significant Investment In Research, Development, And Implementation, As Well As The Re-Education Of Professionals In The Field. Additionally, Some Post-Quantum Algorithms May Have Larger Key Sizes Or Require More Computational Resources Than Their Classical Counterparts, Potentially Impacting The Performance Of Certain Systems And Devices.

Despite These Challenges, The Importance Of Transitioning To Post-Quantum Cryptography Cannot Be Overstated. As Quantum Computing Technology Continues To Advance, The Potential For Devastating Attacks On Our Digital Infrastructure Grows Ever More Imminent. The Development And Adoption Of Post-Quantum Cryptographic Algorithms Are Essential To Ensuring The Continued Security Of Our Digital Lives In The Face Of This Rapidly Evolving Threat Landscape.

In Conclusion, The Rise Of Post-Quantum Cryptographic Algorithms Marks A Critical Turning Point In The World Of Data Security. As Quantum Computing Technology Continues To Advance, It Is Imperative That We Adapt Our Encryption Methods To Withstand The Power Of These Next-Generation Machines. Through The Ongoing Efforts Of Researchers, Industry Experts, And Organizations Such As Nist, We Are Well On Our Way To Ushering In A New Era Of Encryption That Promises To Safeguard Our Digital Assets And Communications In A Quantum World. The Future Of Data Security Depends On Our Ability To Embrace And Implement These Cutting-Edge Cryptographic Techniques, Ensuring That Our Digital Lives Remain Secure For Generations To Come.

3.Quantum Computers Could Break The Internet. Here's How To Save It

by Emily Conover
https://www.sciencenews.org/article/quantum-computers-break-internet-save

Keeping secrets is hard. Kids know it. Celebrities know it. National security experts know it, too.

And it's about to get even harder.

There's always someone who wants to get at the juicy details we'd rather keep hidden. Yet at every moment, untold volumes of private information are zipping along internet cables and optical fibers. That information's privacy relies on encryption, a way to mathematically scramble data to prevent any snoops from deciphering it — even with the help of powerful computers.

But the mathematical basis of these techniques is under threat from a foe that has, until recently, seemed hypothetical: quantum computers.

In the 1990s, scientists realized that these computers could exploit the weird physics of the minuscule realm of atoms and electrons to perform certain types of calculations out of reach for standard computers. That means that once the quantum machines are powerful enough, they could crack the mathematical padlocks on encrypted data, laying bare the world's secrets.

Today's quantum computers are far too puny to defeat current security measures. But with more powerful quantum machines being regularly rolled out by the likes of IBM and Google, scientists, governments and others are beginning to take action. Experts are spreading the word that it's time to prepare for a milestone some are calling Y2Q. That's the year that quantum computers will gain the ability to crack the encoding schemes that keep electronic communications secure.

"If that encryption is ever broken," says mathematician Michele Mosca, "it would be a systemic catastrophe."

Y2Q is coming. What does it mean?

Encryption pervades digital life — safeguarding emails, financial and medical data, online shopping transactions and more. Encryption is also woven into a plethora of physical devices that transmit information, from cars to robot vacuums to baby monitors. Encryption even secures infrastructure such as power grids. The tools Y2Q threatens are everywhere. "The stakes are just astronomically high," says Mosca, of the University of Waterloo in Canada, who is also CEO of the cybersecurity company evolutionQ.

The name Y2Q alludes to the infamous Y2K bug, which threatened to create computer havoc in the year 2000 because software typically used only two digits to mark the year (*SN: 1/2/99, p. 4*). Y2Q is a similarly systemic issue, but in many ways, it's not a fair comparison. The fix for Y2Q is much more complex than changing how dates are represented, and computers are now even more inextricably entwined into society than two decades ago. Plus, no one knows when Y2Q will arrive.

Confronted with the Y2Q threat, cryptography — the study and the practice of techniques used to encode information — is facing an overhaul. Scientists and mathematicians are now working urgently to

prepare for that unknown date by devising new ways of encrypting data that won't be susceptible to quantum decoding. An effort headed by the U.S. National Institute of Standards and Technology, or NIST, aims to release new standards for such post-quantum cryptography algorithms next year.

Meanwhile, a longer-term effort takes a can't-beat-'em-join-'em approach: using quantum technology to build a more secure, quantum internet. Scientists around the world are building networks that shuttle quantum information back and forth between cities, chasing the dream of communication that theoretically could be immune to hacking.

How public-key cryptography works

If you want to share a secret message with someone, you can encrypt it, garbling the information in such a way that it's possible to decode it later.

Schoolkids might do this with a simple cipher: For example, replace the letter A with the number 1, B with 2 and so on. Anyone who knows this secret key used to encrypt the message can later decode the message and read it — whether it's the intended recipient or another sneaky classmate.

It's a simplified example of what's called symmetric-key cryptography: The same key is used to encode and decode a message. In a more serious communication, the key would be much more complex — essentially impossible for anyone to guess. But in both cases, the same secret key is used to encode and decode.

This strategy was used in cryptography for millennia, says computer scientist Peter Schwabe of the Max Planck Institute for Security and Privacy in Bochum, Germany. "It was either used in a military context or it was used between lovers that were not supposed to love each other."

But in the globally connected modern world, symmetric-key cryptography has a problem. How do you get the secret key to someone on the other side of the planet, someone you've never met, without anyone else getting their hands on it?

To solve this quandary, in the 1970s cryptographers devised public-key cryptography, which uses special mathematical tricks to solve the symmetric-key conundrum. It uses two different, mathematically related keys. A public key is used to encrypt messages, and a mathematically related private key decodes them. Say Alice wants to send a message to Bob. She looks up his public key and uses it to scramble her communication. Only Bob, with his private key, can decode it. To any snoops that intercept the message, it's meaningless.

Public-key techniques are also used to create digital signatures. These signatures verify that someone online really is who they say they are, so you know you're really downloading that new app from Apple, not some nefarious impersonator. Only the owner of a private key can sign the message, but anyone can use the public key to verify its authenticity.

The public-key cryptography that permeates the internet is directly vulnerable to full-scale quantum computers. What's more, symmetric-key cryptography often relies on public-key cryptography to share the secret key needed to communicate. That puts the majority of internet security under threat.

Why quantum computers will threaten public-key cryptography

If public-key encryption keeps your data hidden away under the floorboards, then to read that information, you need to build a way in. You have to be able to access the data with your private key. "There's got to be a secret door somewhere in there, where if I knock the right way, it opens up," Mosca says.

Constructing such a trapdoor demands special mathematical tactics, based on operations that are easy to perform in one direction but hard in the opposite direction. Multiplying two prime numbers together is quick work for a computer, even if the numbers are very large. But it's much more time-consuming for a computer to calculate the primes from their product. For large enough numbers, it's impossible to do in a practical amount of time with a standard computer.

The challenge of finding the prime factors of a large number is behind one of the main types of public-key encryption used today, known as RSA. A hacker using a classical computer wouldn't be able to deduce the private key from the public key. Another math problem, known as the discrete logarithm problem, is a similar one-way street.

These two mathematical problems underlie nearly all of the public-key cryptography in use today. But a sufficiently powerful quantum computer would blow their trapdoors wide open. "All of those public-key algorithms are vulnerable to an attack that can only be carried out by a quantum computer," says mathematician Angela Robinson of NIST, in Gaithersburg, Md. "Our whole digital world is relying on quantum-vulnerable algorithms."

This vulnerability came to light in 1994, when mathematician Peter Shor, now at MIT, came up with an algorithm that would allow quantum computers to solve both of these math problems. In quantum machines, the bits, called qubits, can take on values of 0 and 1 simultaneously, a state known as a superposition. And qubits can be linked with one another through the quantum connection called entanglement, enabling new tactics like Shor's (*SN: 7/8/17 & 7/22/17, p. 34*).

"Back then, that was an interesting theoretical paper. Quantum computers were a distant dream," says mathematician Dustin Moody of NIST, "but it wasn't a practical threat." Since then, there's been a quantum computing boom (*SN: 7/8/17 & 7/22/17, p. 28*).

The machines are being built using qubits made from various materials — from individual atoms to flecks of silicon to superconductors (which conduct electricity without resistance) — but all calculate according to quantum rules. IBM's superconducting quantum computer Osprey, for example, has 433 qubits. That's up from the five qubits of the computer IBM unveiled in 2016. The company plans to roll out one with more than a thousand qubits this year.

That's still far from the Y2Q threshold: To break RSA encryption, a quantum computer would need 20 million qubits, researchers reported in 2021 in *Quantum*.

Mosca estimates that in the next 15 years, there's about a 50 percent chance of a quantum computer powerful enough to break standard public-key encryption. That may seem like a long time, but experts estimate that previous major cryptography overhauls have taken around 15 years. "This is not a Tuesday patch," Mosca says.

The threat is even more pressing because the data we send today could be vulnerable to quantum computers that don't exist yet. Hackers could harvest encrypted information now, and later decode it once a powerful quantum computer becomes available, Mosca says. "It's just bad news if we don't get ahead of this."

New algorithms could safeguard our security

Getting ahead of the problem is the aim of Moody, Robinson and others who are part of NIST's effort to select and standardize post-quantum encryption and digital signatures. Such techniques would have to thwart hackers using quantum machines, while still protecting from classical hacks.

After NIST put out a call for post-quantum algorithms in 2016, the team received dozens of proposed

schemes. The researchers sorted through the candidates, weighing considerations including the level of security provided and the computational resources needed for each. Finally, in July 2022, NIST announced four schemes that had risen to the top. Once the final standards for those algorithms are ready in 2024, organizations can begin making the post-quantum leap. Meanwhile, NIST continues to consider additional candidates.

In parallel with NIST's efforts, others are endorsing the post-quantum endeavor. In May 2022, the White House put out a memo setting 2035 as the goal for U.S. government agencies to go post-quantum. In November, Google announced it is already using post-quantum cryptography in internal communications.

Several of the algorithms selected by NIST share a mathematical basis — a technique called lattice-based cryptography. It relies on a problem involving describing a lattice, or a grid of points, using a set of arrows, or vectors.

In math, a lattice is described by a set of vectors used to produce it. Consider Manhattan. Even if you'd never seen a map of the city, you could roughly reproduce its grid using two arrows, one the length and direction of an avenue block and the other matching a street block. Discounting the city's quirks, such as variations in block lengths, you'd just place arrows end-to-end until you've mapped out the whole grid.

But there are more complicated sets of vectors that can reproduce the city's grid. Picture two arrows starting, for example, at Washington Square Park in lower Manhattan, with one pointing to Times Square in Midtown and the other to a neighboring landmark, the Empire State Building. Properly chosen, two such vectors could also be used — with more difficulty — to map out the city's grid.

A math problem called the shortest vector problem asks: Given a set of long vectors that generate a lattice, what is the shortest vector that can be used as part of a set to produce the grid? If all you knew about the city was the location of those three landmarks, it'd be quite a task to back out the shortest vector corresponding to the city's blocks.

Now, picture doing that not for a 2-D map, but in hundreds of dimensions. That's a problem thought to be so difficult that no computer, quantum or classical, could do it in a reasonable amount of time.

The difficulty of that problem is what underlies the strength of several post-quantum cryptography algorithms. In lattice-based cryptography, a short vector is used to create the private key, and the long vectors produce the public key.

Other post-quantum schemes NIST considered are based on different math problems. To choose among the options, NIST mathematicians' chief consideration was the strength of each algorithm's security. But none of these algorithms are definitively proved to be secure against quantum computers, or even classical ones. One algorithm originally considered by NIST, called SIKE, was later broken. It took just 10 minutes to crack on a standard computer, researchers reported in April in *Advances in Cryptology – EUROCRYPT 2023*.

Although it might seem like a failure, the SIKE breakdown can be considered progress. The faith in the security of cryptographic algorithms comes from a trial by fire. "The more [that] smart people try to break something and fail, the more confidence we can get that it's actually hard to break it," Schwabe says. Some algorithms must perish in the process.

A quantum internet could bolster security

Quantum physics taketh away, but also, it gives. A different quantum technique can allow communication with mathematically proved security. That means a future quantum internet could, theoretically at

least, be fully safe from both quantum and classical hacks.

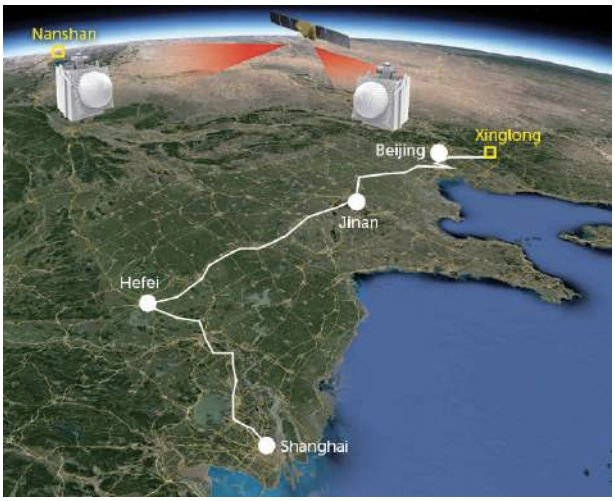
By transmitting photons — particles of light — and measuring their properties upon arrival, it's possible to generate a shared private key that is verifiably safe from eavesdroppers.

This quantum key distribution, or QKD, relies on a principle of quantum physics called the no-cloning theorem. Essentially, it's impossible to copy quantum information. Any attempt to do so will alter the original information, revealing that someone was snooping. "Someone who was trying to learn that information would basically leave a fingerprint behind," says quantum engineer Nolan Bitner of Argonne National Laboratory in Lemont, Ill.

This quirk of quantum physics allows two people to share a secret key and, by comparing notes, determine whether the key has been intercepted along the way. If those comparisons don't match as expected, someone was eavesdropping. The communicators discard their key and start over. If there is no sign of foul play, they can safely use their shared secret key to encrypt their communication and send it over the standard internet, certain of its security. It's a quantum solution to the quandary of how two parties can share secret keys without ever meeting. There's no need for a mathematical trapdoor that might be vulnerable to an undiscovered tactic.

But QKD can't be done over normal channels. It requires quantum networks, in which photons are created, sent zipping along optical fibers and are manipulated at the other end.

Such networks already snake through select cities in the world. One threads through Chicago suburbs from the University of Chicago to Argonne lab and Fermilab in Batavia, for a total of 200 kilometers. In China, an extensive network connects cities along a more than 2,000-kilometer backbone that wends from Beijing to Shanghai, along with two quantum satellites that beam photons through the air. A quantum network crisscrosses South Korea, and another links several U.K. cities. There are networks in Tokyo and the Netherlands — the list goes on, with more to come.



Many of these networks are test-beds used by researchers to study the technology outside of a lab. But some are getting real-world use. Banks use China's network, and South Korea's links government agencies. Companies such as ID Quantique, based in Switzerland, offer commercial QKD devices.

QKD's security is mathematically proven, but quantum networks can fall short of that guarantee in practice. The difficulty of creating, transmitting, detecting and storing quantum particles can open loopholes. Devices and networks must be painstakingly designed and tested to ensure a hacker can't game the system.

And one missing component in particular is holding quantum networks back. “The number one device is quantum memory,” says quantum physicist Xiongfeng Ma of Tsinghua University in Beijing. When sending quantum information over long distances through fibers, particles can easily get lost along the way. For distances greater than about 100 kilometers, that makes quantum communication impractical without the use of way stations that amplify the signal. Such way stations temporarily convert data into classical, rather than quantum, information. That classical step means hackers could target these “trusted nodes” undetected, marring QKD’s pristine security. And it limits what quantum maneuvers the networks can do.

It’s not possible to create pairs of particles that are entangled over long distances in a network like this. But special stations sprinkled throughout the network, called quantum repeaters, could solve the problem by storing information in a quantum memory. To create far-flung entangled particles, scientists could first entangle sets of particles over short distances, storing them in quantum memories at each quantum repeater. Performing certain operations on the entangled particles could leapfrog that entanglement to other particles farther apart. By repeating this process, particles could be entangled across extended distances.

But, thanks in part to quantum particles’ tendency to be easily perturbed by outside influences, scientists have yet to develop a practical quantum repeater. “When that does appear, it’s likely to catalyze global quantum networks,” says David Awschalom, a physicist at the University of Chicago. Not only will such technologies allow longer distances and better security for QKD, but they will also enable more complicated tasks, like entangling distant quantum computers to allow them to work together.

A European effort called the Quantum Internet Alliance aims to build a network with quantum repeaters by the end of 2029, creating a backbone stretching over 500 kilometers, in addition to two metropolitan-scale networks. The effort is “super challenging,” says physicist and computer scientist Stephanie Wehner of Delft University of Technology in the Netherlands. “We are on a moon shot mission.” Eventually, scientists envision a global quantum internet.

Awschalom imagines the networks becoming accessible to all. “Wouldn’t it be great to be able to go to a public library and be able to get onto a quantum network?”

What does the future of cryptography look like?

QKD and post-quantum cryptography are complementary. “In order to overcome the threat of the quantum computers we need both,” says physicist Nicolas Gisin of the University of Geneva and cofounder of ID Quantique. When people are exchanging information that doesn’t require the utmost security — say, using a mobile phone to post cat memes on Reddit — post-quantum cryptography will be more practical, as it doesn’t demand a to-and-fro of individual quantum particles. But “there are really situations where we want to make sure that the security is going to last … for several decades, and post-quantum cryptography cannot guarantee that,” Gisin says.

Eventually, quantum techniques could allow for even more advanced types of security, such as blind quantum computing. In that scheme, a user could compute something on a remote quantum computer without anyone being able to determine what they’re computing. A technique called covert quantum communication would allow users to communicate securely while hiding that they were exchanging messages at all. And device-independent QKD would ensure security even if the devices used to communicate are potentially flawed (*SN: 8/27/22, p. 10*).

The appeal of such extreme secrecy, of course, depends upon whether you’re the secret-keeper or the snoop. In the United States, government agencies like the FBI, CIA and the National Security Agency have argued that encryption makes it difficult to eavesdrop on criminals or terrorists. The agencies have

a history of advocating for back doors that would let them in on encrypted communications — or building in secret back doors.

But quantum techniques, done properly, can prevent anyone from intercepting secrets, even powerful government agencies.

“It’s interesting to think about a world where, in principle, one might imagine perfect security,” Awschalom says. “Is that a good thing or is that a bad thing?”

4.How Important Is Cryptography Knowledge in the Work of an IT Project Manager?

by Micah Abiodun
https://www.cryptopolitan.com/cryptography-knowledge-it-project-manager/

As technology continues to advance at an unprecedented rate, the significance of data security in the information technology sphere cannot be overstated. Amidst this evolving digital landscape, an IT Project Manager’s role becomes increasingly multifaceted, with a growing emphasis on not just overseeing the project’s implementation but also ensuring the security and integrity of data involved. An important skill set in this context is a thorough understanding of cryptography.

This article explores the relevance of cryptography knowledge in an IT Project Manager’s work, elucidating why this skill is necessary, how it can enhance an IT Project Manager’s performance, and the potential benefits of specializing in this field.

Understanding Cryptography

Cryptography is the science of encoding and decoding messages to maintain their confidentiality and integrity. It acts as a fortress of secure communication, shielding data from the prying eyes of malicious entities, referred to as adversaries. The essence of cryptography lies in encryption, a process that employs a unique key and a specific algorithm to convert plaintext, the original message, into ciphertext, the encrypted message. The core strength of an encryption algorithm is its ability to generate identical ciphertext from the same plaintext, given the same key is used. The real test of an encryption algorithm’s security is its resistance against adversaries who have access to the ciphertext but are unable to decipher any information about the plaintext or key.

The Significance of Cryptography

Cryptography is an essential tool in tackling a multitude of security challenges. Its central role is to ensure the confidentiality, integrity, and availability of data, as well as establish authenticity and non-repudiation. Cryptography aids in safeguarding data in transit and at rest, authenticating communication partners, and ensuring non-repudiation, preventing a party from denying previous actions.

In the context of software systems, interactions often occur between multiple endpoints, such as numerous clients and back-end servers, over networks whose trustworthiness is uncertain. These communications could happen via public networks like the Internet, or private networks vulnerable to external

and internal attacks.

Cryptography serves as a shield against two primary types of network attacks: passive and active. Passive attacks encompass an attacker silently observing network activity, aiming to access sensitive information. This can occur online, with the attacker reading real-time traffic, or offline, where the attacker captures real-time traffic to decipher later. Active attacks, on the other hand, involve an attacker intercepting communications, impersonating a client or server, and possibly manipulating the contents before re-transmission.

Through cryptographic protocols such as SSL/TLS, communications are safeguarded from eavesdropping and tampering, ensuring confidentiality and integrity. They also verify user authenticity, confirming the legitimacy of the communication parties. Additionally, cryptography can safeguard data at rest, encrypting sensitive data to prevent unauthorized access in case of physical media loss or theft. It also offers integrity protection, enabling detection of malicious tampering.

Importance of Cryptography Knowledge in the Work of an IT Project Manager

As an IT Project Manager, you act as the bridge between the client and the development team, driving the ideation, execution, and final delivery of the project. This role involves handling confidential information, assessing and managing risks, and ensuring that project objectives align with the client's needs. Cryptography plays a critical role in all these areas. Here's how:

Ensuring Data Security and Privacy

Data security is the bedrock of all IT-related projects. Given the significance and sensitive nature of the data you handle as a Project Manager, it is essential to ensure its safety. It's not just about the security of project documents; the products or services your team develops must also be robust against security breaches. Understanding cryptographic techniques can help you assess potential vulnerabilities and implement suitable encryption methods to secure the data.

Consider the spectrum of threats, from DoS and DDoS attacks to malware, web defamation, spam, and e-mail phishing attacks. With cryptographic knowledge, you can foresee these potential threats, enforce proper security measures, and ensure the use of secure communication channels. You can also educate your team and the client about secure practices, further minimizing risks.

Achieving Regulatory Compliance

Many industries operate under stringent regulatory requirements to ensure data security. Compliance to these requirements is not optional; it's a business necessity. Your understanding of cryptographic standards can be critical in adhering to such requirements. Around 90% of organizations leverage cryptographic standards in their product design and testing. If you can interpret and apply these standards effectively, you can steer your team's work towards compliance, avoiding potential legal and financial repercussions.

Preventing Identity Theft and Fraud

The information exchanged in IT projects often has commercial value. Its leakage could not only cause financial loss but also lead to identity theft and fraud. A comprehensive understanding of encryption and secure communication systems can help mitigate these risks. By selecting the appropriate encryption programs and secure systems for communication, you can thwart unauthorized access and ensure the integrity and confidentiality of your information.

Encryption in Software Development

Your role extends to the nitty-gritty of project execution, where cryptography plays an even bigger role. The encryption algorithms used in software development significantly affect product functionality and performance. While asymmetric algorithms may offer more security, they demand more operational memory and time for data encryption. On the other hand, the symmetric AES algorithm may require higher transmission bandwidth, which could increase costs. Understanding these nuances allows you to make informed decisions about the suitable encryption models for your project, optimizing functionality, security, and cost.

Secure Communication in Project Teams

As the primary communication hub in your project, you need to establish secure communication channels among team members. Knowledge of cryptography empowers you to select and implement secure communication platforms, thus preventing unauthorized access to sensitive project details. Additionally, you can guide your team on how to use these platforms securely, reinforcing the project's overall security.

Use of Digital Signatures and Certificates

Digital signatures and certificates are crucial in validating the authenticity of data and establishing trust in digital environments. As an IT project manager, understanding how these cryptographic tools work enables you to implement them in your projects, enhancing the credibility and integrity of your digital assets. Furthermore, it helps in setting up secure virtual workflows, a necessity in today's remote and hybrid working models.

As an IT Project Manager, your proficiency in cryptography is a significant asset. Not only does it enable you to safeguard sensitive information, but it also empowers you to make informed decisions about the security aspects of your project, ensuring efficient and secure project execution. Additionally, you can provide clients with more insightful consultations and foster a safer digital environment for your team. With knowledge of cryptography, you're well-equipped to handle the dynamic challenges of the IT landscape.

Is Specializing in Cryptography a Good Career Move for IT Project Managers?

When considering the rapidly changing technological landscape and the increasing importance of data security, one might wonder if specializing in a niche area like cryptography would be a strategic career move for an IT project manager. This section will delve into the key reasons why pursuing expertise in cryptography could indeed be a powerful addition to an IT project manager's skill set.

Increasing Demand for Security Knowledge

The ever-evolving threat landscape is driving a surge in demand for professionals who understand how to protect data and systems. The adoption of digital solutions across sectors is growing exponentially, consequently increasing the potential attack surface for cybercriminals. As organizations become more aware of the importance of securing their digital assets, the demand for project managers who can navigate the complexities of secure system design and deployment is growing. An understanding of cryptographic principles can enhance an IT project manager's ability to deliver such secure solutions.

Competitive Advantage

Specializing in cryptography could provide an IT project manager with a unique competitive advantage.

In a world where privacy and data protection are becoming fundamental business imperatives, an IT project manager with a strong understanding of cryptography stands out. This knowledge can be a distinguishing factor in job applications, promotions, and even while pitching for projects, making it an invaluable career investment.

Expanded Career Opportunities

The field of cryptography isn't just about code and algorithms; it is increasingly becoming central to numerous areas of technology. From securing network communications and cloud data storage, to ensuring transaction integrity in blockchain technology and enabling secure user authentication in IoT devices, cryptography has wide-ranging applications. This breadth opens up new avenues and opportunities for IT project managers, extending their potential career paths beyond traditional roles.

Deepening Trust with Stakeholders

A project manager with deep cryptographic knowledge can increase trust among stakeholders, including clients and team members. Being able to articulate how you're protecting their information or why a certain security protocol is in place can be reassuring to those who are entrusting you with their valuable resources. It demonstrates your commitment to their security and can go a long way in fostering stronger, more enduring professional relationships.

Personal Development and Satisfaction

On a personal level, gaining a deep understanding of cryptography can be intellectually satisfying. It can stimulate problem-solving and critical thinking skills, qualities that are beneficial for any project manager. The challenge of keeping up with the fast-paced developments in this field can be a rewarding endeavor, contributing to personal growth and development.

Conclusion

In this age of digital transformation, cryptography has emerged as a crucial skill set for IT Project Managers. A thorough understanding of cryptography is integral to the role, as it enables managers to handle confidential information securely, adhere to regulatory compliance, prevent identity theft and fraud, and manage secure communication within project teams.

As technology continues to evolve, and as the threats to data security become more sophisticated, the importance of cryptography in project management will only increase. Specializing in cryptography not only offers project managers a competitive edge but also opens up new avenues of opportunity, increasing their relevance and versatility in a rapidly evolving professional landscape.

5.IBM: Quantum Computers Are Already Doing Heavy Lifting

by Charles Q. Choi
https://spectrum.ieee.org/practical-quantum-computing-ibm

As powerful as quantum computers may theoretically one day be, they are currently so prone to error that their ultimate utility is often questioned. Now, however, IBM argues that quantum computing may be

entering a new era of utility sooner than expected, with its 127-qubit Eagle quantum computer potentially delivering accurate results on useful problems beyond what even today's supercomputers can tackle.

Quantum computers can in theory find answers to problems that classical computers would take eons to solve. The more components, known as quantum bits or qubits, that a quantum computer has linked together, the more basic computations, known as quantum gates, it can perform, in an exponential fashion.

The key problem that quantum computers face is how notoriously vulnerable they are to disruption from the slightest disturbance. Present-day state-of-the-art quantum computers typically suffer roughly one error every 1,000 operations, and many practical applications demand error rates lower by a billionfold or more.

Scientists hope to one day build so-called fault-tolerant quantum computers, which can possess many redundant qubits. This way, even if a few qubits fail, quantum error-correction techniques can help quantum computers detect and account for these mistakes.

However, existing quantum computers are so-called noisy intermediate-scale quantum (NISQ) platforms. This means they are too error ridden and possess too few qubits to successfully run quantum error-correction techniques.

Despite the current early nature of quantum computing, previous experiments by Google and others claimed that quantum computers may have entered the era of "quantum advantage," "quantum primacy," or "quantum supremacy" over typical computers. Critics in turn have argued that such tests showed only that quantum computers were able to outperform classical machines on contrived problems. As such, it remains hotly debated whether quantum computers are good enough to prove useful right now. Now IBM reveals that its Eagle quantum processor can accurately simulate physics that regular computers find difficult to model past a certain level of complexity. Not only are these simulations of actual use to researchers, the company says, but the methods they developed could be applied to other kinds of algorithms running on quantum machines today.

In experiments, the researchers had IBM's quantum computer model the dynamics of the spins of electrons in a material to predict its properties, such as magnetization. This model is one that scientists understand well, making it easier for the researchers to validate the correctness of the quantum computer's results.

"Importantly, our methods are not limited to this particular model," says study coauthor Kristan Temme, a quantum physicist at IBM's Thomas J. Watson Research Center, in Yorktown Heights, New York. "These methods can be applied to other, more general circuits."

At the same time, scientists at the University of California, Berkeley, performed versions of these simulations on classical supercomputers to compare how well the quantum computer performed. They used two sets of techniques. Brute-force simulations provided the most accurate results, but also demanded too much processing power to simulate large, complex systems. On the other hand, approximation methods could estimate answers for big systems, but they generally prove less and less accurate the larger a system gets.

At the largest scale examined, the quantum computer was roughly three times as fast as the classical approximation methods, finding answers in nine hours compared to 30. More importantly, the researchers found that as the scale of the models increased, the quantum computer matched the classical brute-force simulations, while the classical approximation methods became less accurate.

"What we are doing in this work is to demonstrate that we can run quantum circuits at a very large scale and get correct results, something that has always been called into question and for which many people

argued would be not feasible on the current devices," Temme says.

When comparisons showed the quantum results did not agree with the classical approximation methods, "we initially assumed that the experiment had made a mistake," Temme says. It was "quite the surprise to then learn" that the quantum computer matched the classical brute-force simulations rather than the classical approximation methods, he adds.

The scientists conducted tests in which they generated results from 127 qubits running 60 steps' worth of 2,880 quantum gates. They note that what a quantum computer can theoretically do with 68 qubits is already beyond what classical brute-force simulations are capable of calculating. Although the researchers cannot prove whether the answers the quantum computer provided when using more than 68 qubits are correct, they argue that its success on previous runs makes them confident it was.

The IBM scientists caution that they are not claiming their quantum computer is better than classical computing. Future research may soon find that regular computers may find correct answers for the calculations used in these experiments, they say.

"We hope that this will lead to a back-and-forth between methods, which the quantum computer will ultimately win," Temme says.

In any case, even if quantum computers do not completely outcompete classical computers—yet—these new findings suggest they may still prove useful for problems that regular computers find extraordinarily difficult. This suggests we may now be entering a new era of utility for quantum computing, Darío Gil, senior vice president and director of IBM Research, said in a statement.

IBM notes that its quantum hardware displayed more stable qubits and lower error rates than it did previously. However, the new findings depended on what IBM calls "quantum error mitigation" techniques, which examine a quantum computer's output to account for and eliminate noise that its circuits experienced.

The quantum error mitigation strategy that IBM used in the new study, zero-noise extrapolation, repeated quantum computations at varying levels of noise the quantum processor may have experienced from its environment. This helped the researchers extrapolate what the quantum computer would have calculated in the absence of noise.

"Both our hardware and our error-mitigation methods are now at the level they can be used to start implementing the overwhelming majority of all the near-term algorithms that have been proposed in the last five to 10 years, to see which algorithm actually provides a quantum advantage in practice," Temme says.

One drawback of zero-noise extrapolation is that it does require a quantum computer to run its circuits multiple times. "For the zero-noise extrapolation method we have used here, we need to run the same experiment at three different noise levels," Temme says. "This is a cost that has to be paid for every data point in the calculation—that is, each time we use the processor."

IBM notes that these new findings represent early results on quantum error mitigation at this scale. "We think there still is quite a bit of room for improvement in these methods," Temme says. Future research can also test if quantum error mitigation can apply generally, as the company hopes, to other kinds of quantum applications beyond this one model, he adds.

IBM says its quantum computers running both on the cloud and on-site at partner locations in Japan, Germany, and the United States will be powered by a minimum of 127 qubits over the course of the next year.

"Ultimately, we will want to have a fault-tolerant quantum computer," Temme says. "The long-term direction has to be to bridge these results all the way up to a point where we can use quantum error correction. We expect this to drive the hardware development, where every component-wise improvement now translates to more complex calculations that can be run, leading to a smoother transition to a fault-tolerant device."

The scientists detailed their findings 14 June in the journal *Nature*.

6.IDQ Europe Becomes Nutshell Quantum-Safe

by Matt Swayne
https://thequantuminsider.com/2023/06/21/idq-europe-becomes-nutshell-quantum-safe/

ID Quantique Europe GmbH (IDQ Europe), a developer and provider of Quantum Key Distribution (QKD) solutions in Vienna, Austria, is becoming Nutshell Quantum-Safe GmbH. Aiming at supplying QKD network solutions to protect European data in transit, the company supports national and European QKD initiatives and contributes to building a leading and sustainable quantum industry in the EU.

QKD is a technology to permanently protect data in transit – even against attackers using the most powerful quantum computers now and in the future. The European Commission and the Union's member states have recognized this potential and initiated programs, like the European Quantum Communication Infrastructure (EuroQCI), to develop and deploy QKD networks for the future-proof protection of its critical infrastructure.

Today, the EU needs a coordinated effort to develop, certify, deploy and accredit the necessary QKD infrastructures throughout its 27 members. At the same time, it wants to avoid new dependencies from companies and countries outside the EU. However, while some pioneering companies have developed QKD in Europe, the EU-based QKD industry itself is today at an early stage, implying a risk that the joint goal may not be reached in time.

In 2021, the Swiss company ID Quantique, a world leader in QKD development and commercialization, decided to spin off the Austrian company IDQ Europe to make its pioneering QKD technology available to the European governmental market in a compliant way. Today, IDQ Europe is fully owned and controlled within the EU. The independence from ID Quantique is now underlined with this new distinguishable branding.

Nutshell Quantum-Safe has set up its business in Vienna to support the EU's cybersecurity agenda with cutting-edge QKD technology. The company is a value-added reseller of QKD solutions from ID Quantique. With its experienced team, Nutshell offers services like consulting, QKD network project implementation, and technical customer support. The next step is to open an EU-based production of QKD equipment. Furthermore, the company is actively pursuing R&D collaborations on QKD components, systems and network integration with European partners.

According to Dr. Florian Fröwis, CEO of Nutshell Quantum-Safe: "QKD can and should soon yield value to European citizens by protecting private, governmental, and commercial data. Nutshell Quantum-Safe supports the European initiatives to accelerate the availability of advanced and high-value QKD technologies."

Nutshell meaning. The security of QKD is based on the fundamental laws of quantum mechanics. In QKD, single photons are exchanged between distant users. The attempt to read the information carried by the photons by an attacker will necessarily leave a trace that is detectable by the QKD devices. The nutshell symbolizes the protection of the quantum information. Accessing the information is like cracking the nutshell to grab the nut. It is impossible to get the nut without leaving a trace on the nutshell.

7.Researchers develop open-source software to speed up quantum research

by Chalmers University of Technology
https://phys.org/news/2023-06-open-source-software-quantum.html

Quantum technology is expected to fundamentally change many key areas of society. Researchers are convinced that there are many more useful quantum properties and applications to explore than those we know today. A team of researchers at Chalmers University of Technology in Sweden have now developed open-source, freely available software that will pave the way for new discoveries in the field and accelerate quantum research significantly.

Within a few decades, quantum technology is expected to become a key technology in areas such as health, communication, defense and energy. The power and potential of the technology lie in the odd and very special properties of quantum particles.

Of particular interest to researchers in the field are the superconducting properties of quantum particles that give components perfect conductivity with unique magnetic properties. These superconducting properties are considered conventional today and have already paved the way for entirely new technologies used in applications such as magnetic resonance imaging equipment, maglev trains and quantum computer components. However, years of research and development remain before a quantum computer can be expected to solve real computing problems in practice, for example. The research community is convinced that there are many more revolutionary discoveries to be made in quantum technology than those we know today.

Open-source code to explore new superconducting properties

Basic research in quantum materials is the foundation of all quantum technology innovation, from the birth of the transistor in 1947, through the laser in the 1960s to the quantum computers of today. However, experiments on quantum materials are often very resource-intensive to develop and conduct, take many years to prepare and mostly produce results that are difficult to interpret. Now, however, a team of researchers at Chalmers have developed the open-source software SuperConga, which is free for everyone to use, and specifically designed to perform advanced simulations and analyses of quantum components.

The program operates at the mesoscopic level, which means that it can carry out simulations that are capable of "picking up" the strange properties of quantum particles, and also apply them in practice. The open-source code is the first of its kind in the world and is expected to be able to explore completely new superconducting properties and eventually pave the way for quantum computers that can use advanced computing to tackle societal challenges in several areas.

"We are specifically interested in unconventional superconductors, which are an enigma in terms of how they even work and what their properties are. We know that they have some desirable properties that

allow quantum information to be protected from interference and fluctuations. Interference is what currently limits us from having a quantum computer that can be used in practice. And this is where basic research into quantum materials is crucial if we are to make any progress," says Mikael Fogelström, Professor of Theoretical Physics at Chalmers.

These new superconductors continue to be highly enigmatic materials—just as their conventional siblings once were when they were discovered in a laboratory more than a hundred years ago. After that discovery, it would be more than 40 years before researchers could describe them in theory. The Chalmers researchers now hope that their open-source code can contribute to completely new findings and areas of application.

"We want to find out about all the other exciting properties of unconventional superconductors. Our software is powerful, educational and user-friendly, and we hope that it will help generate new understanding and suggest entirely new applications for these unexplored superconductors," says Patric Holmvall, postdoctoral researcher in condensed matter physics at Uppsala University.

Desire to make life easier for quantum researchers and students

To be able to explore revolutionary new discoveries, tools are needed that can study and utilize the extraordinary quantum properties at the minimal particle level, and can also be scaled up large enough to be used in practice. Researchers need to work at mesoscopic scale. This lies at the interface between the microscopic scale, i.e. the atomic level at which the quantum properties of the particles can still be utilized, and the macroscopic scale which measures everyday objects in our world which, unlike quantum particles, are subject to the laws of classical physics.

On account of the software's ability to work at this mesoscopic level, the Chalmers researchers now hope to make life easier for researchers and students working with quantum physics.

"Extremely simplified models based on either the microscopic or macroscopic scale are often used at present. This means that they do not manage to identify all the important physics or that they cannot be used in practice. With this free software, we want to make it easier for others to accelerate and improve their quantum research without having to reinvent the wheel every time," says Tomas Löfwander, Professor of Applied Quantum Physics at Chalmers.

The article, "SuperConga: An open-source framework for mesoscopic superconductivity," has been published in Applied Physics Reviews and was written by Patric Holmvall, the Department of Physics and Astronomy, Uppsala University, and Niclas Wall Wennerdal, Mikael Håkansson, Pascal Stadler, Oleksii Shevtsov, Tomas Löfwander and Mikael Fogelström, the Department of Microtechnology and Nanoscience at Chalmers University of Technology, Sweden.

More on the microscopic, mesoscopic and macroscopic scales

The mesoscopic regime is at the interface between the macroscopic and microscopic regimes. In the macroscopic regime (typically millimeters and larger), classical physics dominates, describing everyday objects such as footballs, cats or perhaps a coffee maker. This contrasts with the microscopic regime, where quantum physics prevails, and much smaller objects can be measured, such as electrons, atoms and other particles.

The odd properties of quantum particles can be explored on this tiny scale—properties that allow them to be in two places at once or to be perfectly conducting. Mesoscopic quantum components (typically micrometers down to nanometers) are so small that the strange properties of quantum particles can be accessed and used, but also large enough that they can be applied in practice. Open-source codes already exist for simulations at either the microscopic or more macroscopic level. SuperConga is the first

freely available software in the world capable of simulating superconductors at the mesoscopic level.

8.Long-Range Quantum Cryptography Gets Simpler

by Marco Avesani
https://physics.aps.org/articles/v16/104

The secure transmission of data is essential in our interconnected society but is constantly at risk as attackers keep seeking vulnerabilities and new methods to decrypt our messages. The emergence of quantum computers adds to the problem, as they hold the potential to break current encryption methods. A response to these threats is offered by quantum key distribution (QKD)—a cryptography technique exploiting the peculiar laws of quantum mechanics. In QKD, two remote users (Alice and Bob) exploit single photons to generate and exchange cryptographic keys with perfect security, as the activity of any eavesdropper would be spotted through changes in the photons' quantum states. Photon losses, however, limit the speed and distance at which a QKD key can be transmitted, posing a barrier to applications. Some recently demonstrated protocols can in principle overcome these limitations, but at the price of impractically complicated setups. A series of studies, performed by the independent teams of Zhiliang Yuan of the Beijing Academy of Quantum Information and Jan-Wei Pan of the University of Science and Technology of China now shows the possibility of dramatic setup simplifications, removing the need for complex "phase-locking" schemes[1] [2] [3]. Yuan's team's solution, in particular, removes the need for even tracking the phase of the used lasers. It also achieves secure-key transmission up to 500 km at orders-of-magnitude-larger rates than previous demonstrations, approaching values of practical interest. Together, these advances bode well for the transformation of QKD into a broadly available, commercial technology.

QKD—arguably the most mature among quantum technologies—works by exchanging photons between two users via optical fibers or free-space links. Among its biggest enemies are photon losses—due to scattering and absorption—which set the maximum operational distance over which signals aren't trumped by noise. Alas, as of today there is no way to overcome these losses by regenerating signals: optical amplifiers like those used in classical networks would corrupt the quantum signals, while quantum repeaters won't be available any time soon. Point-to-point QKD links over optical fibers have reached up to 421 km (See **Viewpoint: Record Distance for Quantum Cryptography**), but they have impractically low secure-key transmission rates[4].

In 2017, researchers derived a fundamental upper limit to the key-rate transmission of a point-to-point QKD scheme without repeaters (known as the "PLOB" bound from the initials of the paper's authors)[5]. Ever since, however, researchers have proposed alternative QKD protocols that offer improvements in both security and reach without using repeaters. One such protocol, called measurement-device-inde-

[1] L. Zhou *et al.*, "Experimental quantum communication overcomes the rate-loss limit without global phase tracking," **Phys. Rev. Lett. 130, 250801 (2023)**.

[2] H.-T. Zhu *et al.*, "Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking," **Phys. Rev. Lett. 130, 030801 (2023)**.

[3] W. Li *et al.*, "Twin-field quantum key distribution without phase locking," **Phys. Rev. Lett. 130, 250802 (2023)**.

[4] A. Boaron *et al.*, "Secure quantum key distribution over 421 km of optical fiber," **Phys. Rev. Lett. 121, 190502 (2018)**.

[5] S. Pirandola *et al.*, "Fundamental limits of repeaterless quantum communications," **Nat. Commun. 8, 15043 (2017)**.

pendent QKD (MDI-QKD) involves Alice and Bob transmitting photons to an untrusted intermediary (Charlie)[6].

The use of this intermediary implies MDI-QKD can in principle bypass the PLOB bound. But an experimental challenge has so far prevented such a feat. Specifically, MDI-QKD relies on measuring a two-photon interference between photons sent by Alice and Bob and arriving at Charlie's detectors in coincidence. Photon losses and other effects can make such coincident detections unlikely, lowering the secure-key transmission rate. To address this challenge, researchers proposed twin-field QKD (TF-QKD) in 2018 [7]. In TF-QKD, Alice and Bob transmit identical optical fields to Charlie, who measures the interference of fields rather than that of individual photons, eliminating the need for photon coincidence. Several experimental optical-fiber implementations of TF-QKD have indeed circumvented the PLOB bound, reaching 600 km in 2021 [8] and 1000 km in March of this year[9]. However, TF-QKD requires the fields generated by the two distant, independent light sources to be completely identical in every aspect, including their wavelength and the phase the fields acquire after propagation in the fiber. This locking of the system's "global phase" can only be achieved with complex hardware and protocols that hinder applicability in most real-world scenarios. This phase locking usually requires the dissemination of a common optical frequency over long distances. A solution for removing this requirement, based on tracking the phase using optical frequency combs, appeared early this year[10]. The incorporation of frequency combs, however, still introduces significant complexities to the scheme.

In 2022, two independent teams proposed to tackle this problem with a new approach, called post-measurement pairing QKD (PMP-QKD)[11] [12], that combines the best of the MDI- and TF-QKD worlds. The protocol is similar to MDI-QKD but alleviates the photon-coincidence demands. In standard MDI-QKD, photons are only usable if they arrive in two adjacent time bins. In PMP-QKD, Alice and Bob can "pair" their photons after detection, provided that such photons arrive within a so-called "pairing window," whose width is determined by the fiber-induced phase fluctuations and by the rate at which the phases of the two lasers diverge. If this pairing window is sufficiently long, the number of usable photons is larger than that set by the PLOB bound.

Yuan's team and Pan's team demonstrated this PMP protocol experimentally. Both groups utilized a conventional MDI-QKD setup with two independent lasers, a central measurement station (Charlie), and no phase-locking mechanism. The key trick was to ensure a stable and predictable difference in the wavelengths of the two independent lasers, boosting their relative stbility and hence the pairing window's width. The teams exploit different laser technologies. Pan and colleagues employ commercial lasers with a narrow linewidth (about 2 kHz). They then interleave the photon sequences used for quantum communication with bright (classical) reference pulses used to estimate the wavelength difference. In other words, the team removed the need for "locking" the laser phases but "tracked" the phase through the reference pulses. Yuan and colleagues went a step further. They exploited state-of-the-art lasers with an exceptionally narrow (1-Hz) linewidth, which also eliminated the need to track the laser phases.

---

[6] H.-K. Lo *et al.*, "Measurement-device-independent quantum key distribution," **Phys. Rev. Lett. 108, 130503 (2012)**.

[7] M. Lucamarini *et al.*, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," **Nature 557, 400 (2018)**.

[8] M. Pittaluga *et al.*, "600-km repeater-like quantum communications with dual-band stabilization," **Nat. Photon. 15, 530 (2021)**.

[9] Y. Liu *et al.*, "Experimental twin-field quantum key distribution over 1000 km fiber distance," **Phys. Rev. Lett. 130, 210801 (2023)**.

[10] L. Zhou *et al.*, "Twin-field quantum key distribution without optical frequency dissemination," **Nat. Commun. 14, 928 (2023)**.

[11] P. Zeng *et al.*, "Mode-pairing quantum key distribution," **Nat. Commun. 13, 3903 (2022)**.

[12] Y.-M. Xie *et al.*, "Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference," **PRX Quantum 3, 020315 (2022)**.

Pan's team demonstrated a PMP enhancement up to 407 km of optical fibers but didn't break the PLOB bound. Yuan's group, on the other hand, clearly surpassed the PLOB bound at distances of 413 and 508 km, with rates of about 509 and 42 bits/s, respectively. The 5 kbit/s rate they achieved at 306 km—a world's record at this distance—would be sufficient to enable the real-time QKD encryption of voice communications with a secure technique known as one-time pad.

The PMP approach holds potential for wider applicability to other protocols, as shown in a recent study by Pan's group. The team applied a similar phase-estimation and tracking mechanism with bright reference pulses to a TF-QKD scheme. Using commercially available, 5-kHz-linewidth lasers and standard fiber, they surpassed the PLOB bound at 504 km without requiring global phase locking or active phase compensation at the receiver.

The new results show that there is great potential for QKD to become more practical. It is to be expected that there will be swift progress on several fronts—including simpler, less-expensive, and more efficient protocols and devices—which could dramatically boost QKD's appeal for real-world applications.

9.Blueshift makes quantum cryptography connection

by Peter Clarke
https://www.eenewseurope.com/en/blueshift-makes-quantum-cryptography-connection/

Blueshift (Cambridge, England) founded in May 2016, claims to have developed a memory architecture for the superior handling of large data sets and time-critical data. The claim is mde that for applications such as high-performance computing, AI, and AR/VR, Blueshift's 'Cambridge Architecture' for storage can enable 1,000x faster memory access.

Crypta Labs Ltd. (Oxford, England), founded in May 2014, is a developer of a quantum random number generator (QRNG) for resilient encryption.

"Our innovative non-Von Neumann computer architecture already offers a high level of intrinsic cybersecurity," said Peter Marosan, founder and CTO of Blueshift Memory, in a statement. "The solution we are now developing with Crypta Labs adds quantum-resilient protection, meaning that data is encrypted within the memory and can only be read by the CXL-connected CPU. We believe that this joint development will yield one of the first technologies to create a bridge between quantum computing and silicon computer memory technology."

Crypta Labs has developed a discrete Quantum Optics Module (QOM) with embedded software that together constitute QRNG solution. Blueshift Memory said it will integrate the QOM into its Cambridge Architecture FPGA module (see Blueshift Memory wins grant for FPGA development).

"The basis for all encryption starts with a random number, and this is increasingly under attack since many so-called random numbers are in fact created by a pseudo-random generator," said Jose Garcia Coello, chief science officer at Crypta Labs, in the same statement. "By using photons as a source of entropy, we have developed a fast, reliable method to generate true random numbers from that entropy using a quantum optics module. Blueshift Memory has a disruptive technology for highly efficient handling of large data sets and time-critical data like AI, and we are very excited to be working with them to add quantum-resilient cybersecurity to their solution."

As well as developing FPGA IP in 2022 Blueshift Memory was awarded a grant to develop a computer vision AI module based on the Cambridge Architecture and integrating a customized Codasip RISC-V core.

10.WISeKey and SEALSQ Develop AI based Quantum Solutions Demonstrator for Post-Quantum Cryptography

https://www.globenewswire.com/news-release/2023/06/16/2689725/0/en/WISeKey-and-SEALSQ-Develop-AI-based-Quantum-Solutions-Demonstrator-for-Post-Quantum-Cryptography.html

WISeKey International Holding Ltd., a leading global cybersecurity, AI, Blockchain, and semiconductors company, today announced that its subsidiary SEALSQ Corp. has developed using AI Quantum solutions, a demonstrator unit running two NIST selected Post-Quantum Algorithms, a significant milestone for the development of the QUASARS project.

The SEALSQ Post-Quantum engineering team has been able to carry both Kyber and Dilithium CRYSTAL quantum-resistant NIST selected algorithms and the appropriate APIs on the MS6003, a WISeKey Common Criteria EAL5+ Certified secure hardware platform powered by an ARMSC300 core and featuring an USB interface, thus creating the first Quantum-Resistant USB Token demonstrator. The development of this demonstrator marks a significant milestone for the QUASARS project and brings it one step closer towards the goal of building a Post-Quantum Hardware Security Module and Root-of-Trust.

The advent of quantum computers poses a significant challenge to conventional cryptographic methods, such as RSA and Elliptic Curve Cryptography (ECC). As quantum computers continue to advance in power, these methods become vulnerable to quantum attacks, jeopardizing the security of sensitive information. WISeKey's post-quantum solutions, collectively known as Post-Quantum Cryptography (PQC), aim to address this threat by developing cryptographic methods that are resistant to attacks from quantum computers.

WISeKey is developing a new range of Trust Services, that will take advantage of the latest developments in post-quantum encryption (PQE) to be applied in real-world applications of digital signatures and encryption using PKI and digital certificates, such as secure communication channels (TLS), enhanced Key Exchanges and email security (S/MIME). These services are currently based on standards that can be improved to be resilient to quantum attacks and offer backwards compatibility with existing counterparts. WISeKey implementation of PQE is done around the concept of “hybrid signatures” which combine in a single X.509 certificate a conventional signature with a second signature using a PQE algorithm. This approach ensures backwards compatibility and opens a new horizon of cybersecurity services.

WISeKey's AI Quantum solutions mark a significant milestone in the ongoing battle to protect sensitive information from quantum attacks. By combining the power of quantum mechanics and the expertise of our multidisciplinary team, we are confident that these innovations will shape the future of cryptography and cybersecurity. The significance of the semiconductor industry is increasingly profound, not only from a technological standpoint but also strategical one. With the rapidly advancing domain of artificial intelligence (AI), the dependence on sophisticated, high-performance computer chips is growing ever more critical. As AI continues to evolve and innovate, creating transformative tools and applications, it has

started to become a central pillar for the modern economy, business operations, and an array of career paths. Its potential to monetize, particularly in the realm of generative AI, is attracting considerable attention and investment.

AI may appear as if it has taken center stage somewhat abruptly, yet it stands on the shoulders of technologies that have been maturing for decades – the internet, IoT, smartphones, and potent computer chips. Early iterations of AI were primarily centered around automating or expediting tasks, such as chatbots for customer service, automated translation, or enhancing search engine algorithms. These applications served as the bedrock for more advanced AI technologies, driving efficiency and productivity in multiple sectors.

In the realm of autonomous systems, generative AI could drive significant advances. For instance, it can enable cars or robots to make automated decisions, improving safety and efficiency. From self-driving vehicles navigating complex urban environments to industrial robots performing precision tasks, the applications are extensive and game-changing.

For SEALSQ, the intersection of the semiconductor industry and AI signals a crucial inflection point in the digital transformation of our society. The possibilities that lie ahead for generative AI are vast, promising a future where technology further enhances human ingenuity, innovation, and productivity.

11.Are federal agencies' post-quantum cryptography preparations on track?

by Rebecca Heilweil
https://fedscoop.com/are-federal-agencies-post-quantum-cryptography-preparations-on-track/

Today, the government uses standard cryptographic algorithms to protect its data. But amid the rise of quantum computers, these algorithms may not offer the security they once did.

Put simply, quantum computers — with the ability to factor extremely large prime numbers — could one day break into these algorithms, helping adversaries access all sorts of critical information, including personal data about U.S. citizens and critical scientific and military secrets.

"If we can build large-scale quantum computers that run exactly as physics predicts that they should," explains Ryan O'Donnell, a computer science professor at Carnegie Mellon, "then they will be able to break most of the cryptography that was in use up until now."

The danger isn't just a future risk. Researchers — and the government — are also concerned about "store now, decrypt later" attacks. These involve hackers accessing critical federal systems now, and then saving these systems until they can have the quantum computing capabilities to decrypt the data held within them. Even this scenario presents a major security problem, argues Jeremiah Blocki, a Purdue computer science professor who researches password security.

To address this risk, the Office of Management and Budget told federal agencies last November to start preparing. The OMB memo instructed federal agencies to start studying all the systems that may need to be transitioned to post-quantum cryptography (PQC).

By May 4, all federal agencies — excluding the Department of Defense — were supposed to submit an inventory of those systems (and then repeat the process every year) to the Office of the National Cyber

Director and DHS's Cybersecurity and Infrastructure Security Agency (CISA). During this time, they were also supposed to designate a lead to handle the inventory and the PQC migration, among other goals.

But a month after that May 4 deadline, it's not clear how well all federal agencies are keeping up. FedScoop reached out to the more than 20 agencies outlined in the Chief Financial Officers Act, a 1990 law that also spells out the responsibilities of federal chief information officers, and received a range of responses.

Many of those agencies, including the departments of Homeland Security, Commerce Department, and Health and Human Services, did say they were up to date on requirements. But others provided unclear responses about their status. Several agencies, including USAID and the departments of Agriculture and Education, said they were unable to share an update. Other agencies, including the Department of Transportation, the Treasury, and the Social Security Administration, did not respond to repeated requests for comment.

The Department of Housing and Urban Development sent a general statement addressing the agency's investment in IT and cybersecurity improvements but didn't directly address whether its staff had created the required inventory or say that it had designed a migration lead. The Small Business Administration, meanwhile, said that it conducts its inventory "as required," but would only say that a "federal employee" manages the agency's cryptographic inventory.

"Agencies have prioritized their systems for migration to post-quantum cryptography," an OMB official told FedScoop. "OMB and ONCD are working with agencies to ensure accurate cost estimates as we prepare for this transition."

"The consequences associated with the Snowden leaks or the recent Discord leaks would pale in comparison to the consequences associated with agencies' failure to comply with the November 2022 Memo on Migrating to Post-Quantum Cryptography," Sam Howell, a research assistant at the Center for a New American Security's Technology and National Security Program, told FedScoop in an email.

"[It's] important to begin the migration to post-quantum cryptography now because the process could take a long time and entails a lot of challenges," she added.

Building an inventory is a critical first step in preparing for post-quantum cryptography, according to the OMB memo. That inventory is supposed to include systems that an agency uses or that are operated on behalf of that agency, including "high impact information" systems and "high-value assets."

Next, agencies — excluding the Defense Department and intelligence community agencies — were supposed to start preparing funding assessments aimed at estimating how much the post-quantum cryptography (PQC) migration could cost.

The White House wants the federal government to transition to PQC systems by 2035. Still, a June report from the National Quantum Initiative Advisory Committee stated that "an earlier completion date would be highly preferable and should be achievable through vigorous U.S. Government action."

"I don't want to presume to tell a federal agency what data they need to protect or should protect," said Blocki, the computer science professor from Purdue. "But I can imagine that they're going to have a lot of data that remain sensitive even 50 years from now."

12.Quantum Origin Onboard strengthens

device security against cyberattacks

https://www.helpnetsecurity.com/2023/06/14/quantinuum-quantum-origin-onboard/

Quantinuum launched Quantum Origin Onboard, an innovation in cryptographic key generation that provides quantum computing hardened cyber protection for a wide range of connected devices by maximizing the strength of keys generated within the devices themselves.

The risk of cyberattacks compromising organizations continues to grow. As cybercriminals uncover new techniques to exploit connected systems and their data, even the cryptographic foundations of cybersecurity measures remain vulnerable to advanced threats.

Cryptographic keys created using current typical methods deployed by organizations around the world are not provably unpredictable, leaving encrypted data and systems potentially at risk of devastating attacks. Quantinuum's quantum-computing-hardened cryptographic key enhancement solution provably minimizes the risk that businesses generate and use vulnerable encryption keys to protect encrypted data.

"While quantum computing has the potential to render current encryption algorithms obsolete, posing a significant challenge to businesses and individuals alike, already today sophisticated attackers can take advantage of vulnerable encryption keys," said Dr. Rajeeb Hazra, CEO of Quantinuum.

"With our Quantum Origin Onboard and the overall Quantum Origin platform, organizations can fortify defenses across multiple endpoints and embrace the possibilities of a quantum-secure future. The next era of data security is here, and we are proud to be at the forefront as we collaborate with organizations worldwide," added Hazra.

Strengthening encryption at the device level

Quantum Origin Onboard is the first and only commercially available enterprise software solution capable of delivering quantum-computing-hardened key enhancement. It can be installed directly onto devices and used to help deliver unparalleled foundational-level protection.

Quantum Origin Onboard brings enterprise-level security that integrates directly into connected devices without the need for additional hardware upgrades. This unique approach ensures that devices in any environment, online or offline, can generate quantum-computing-hardened keys to continually maximize the strength of encryption measures protecting devices.

Quantum Origin Onboard embeds a quantum seed, created by Quantinuum's H-Series quantum computer, into devices. The seed is a string of provably unpredictable numbers, which enhance a device's capability to generate strong and secure keys.

"Enterprises are recognizing they can build unprecedented resilience by adopting quantum-computing-hardened cryptographic keys," said Duncan Jones, Head of Cybersecurity at Quantinuum. "This is a paradigm shift, and enterprises in critical industries are embracing the opportunity to minimize a risk to one of their attack surfaces, specifically device-level encryption on internet connected products that might be in the field for a decade."

The growing security threat to embedded devices

The growing use of connected devices continues to underpin innovation across industries, from critical

infrastructure to healthcare to transportation to energy. As adoption has risen, cybercriminals have increasingly targeted vulnerable interconnected devices, causing mass disruption.

One of the most infamous examples of the power of IoT-based attacks is the Mirai malware that infected IP cameras and basic home routers, creating a botnet that compromised a leading Domain Name Systems provider, leaving many high-profile websites inaccessible.

Quantum Origin Onboard embeds a security capability into connected devices, to strengthen device security against advanced cyber-attacks, by minimizing an exploitable cyber vulnerability. As the only software solution of its kind, it simplifies deployment and provides uninterrupted key generation for connected devices and the data they manage.

13.Quantum Experts Interviewed on BBC Newsnight about Industry in the UK

by James Dargan
https://thequantuminsider.com/2023/06/14/quantum-experts-interviewed-on-bbc-newsnight-about-industry-in-the-uk/

As part of its ten-year plan to invest in quantum technology this past March, the UK government announced the investment of £2.5 billion into quantum technologies. This news builds on the National Quantum Technologies Programme (NQTP), established nearly a decade ago.

To get more insight into this, BBC Newsnight Science and Technology Correspondent Kate Lamble recently interviewed several UK-based experts in quantum technologies to find out what is happening in the country regarding investment and overall innovation.

NOT FOR FACEBOOK

“So,” it’s not going to speed up Excel, it’s not going to make Facebook run any faster, but it will help us completely revolutionize the way we design new drugs, make them more efficient, optimize logistical networks, or accelerate machine learning,” said Richard Murray, CEO and co-founder of quantum start-up, ORCA Computing, a company that has sold several machines thus far, one to the Ministry of Defence (MoD).

Murray also said the semiconductor sector in the UK is “fairly” well established, adding that there are a few new developments that can be capitalized on, though the key investments and players have been made decades ago.

“Quantum is a completely new industry,” he said. “The game hasn’t been won. And, in fact, the game is just beginning.”

Matt Brookes, a professor of Physics at the University of Nottingham, says that quantum technology has allowed his research to detect the faint magnetic field produced by our brains, pinpointing the exact location of electrical activity, which could have far-reaching effects for conditions like Tourette’s Syndrome and epilepsy.

FRAGILE

“Academia has been driven by the end user, the end goal, so it’s not the case that that you know, we develop a sensor or a system and then try to dole it out to industry and they say it’s no use to us,” said Brookes. “Industry has come in and said this is what we want. And that’s allowed UK academia to actually deliver in perhaps a way that’s not been done before.”

On the topic of UK talent, Brookes thinks the UK quantum technologies program rests on a relatively small number of people, and if these people were to move, then the UK ecosystem would become “fragile”.

“I certainly know people who work with me, who have been given very good offers to go and work in particular to North America,” said Brookes, noting that though the brain drain is not at a critical stage right now, it could be if things don’t change.

Kai Bongs, Director of the DLR Institute for Quantum Technologies, Professor at Ulm University and former Director of UK National Quantum Technology Hub in Sensors and Metrology, stated the UK has been really good at kickstarting the supply chain, though it hasn’t accelerated the market pool as much.

“For that,” he said, “I think we really need to get the right companies on board. There has been a very notable initiative to create a national accelerator for quantum sensors, to look into the energy, defence and communication infrastructures and think about the innovation there, but that definitely needs a program to make it really happen.”

OPEN & END GAME

“I often describe the UK as having a very strong opening game,” Murray added, “but maybe not having so much experience at the late stages of the end game, when it comes to scaling companies up, maintaining market position and things like that. I think quantum is one of the ways that we can change that.”

Michelle Donelan MP, secretary of state for the recently created Department for Science, Innovation, and Technology (DSIT), wrote in a foreword to the strategy:

“This ten-year plan will fund new frontiers of quantum research, support and develop our growing quantum sector, prepare our wider economy for the quantum revolution and ensure that the UK leads internationally in the regulation and ethical use of quantum technologies.

We will make the UK the home for cutting-edge scientific breakthroughs, the best place in the world to start and grow a quantum business, a leading voice in the international quantum and tech community, and a magnet for international quantum talent,” adding that the government firmly believes Britain should lead the world in this physical science and deliver opportunities and jobs in hardware, engineering and advanced manufacturing, as well as in software and applications across the economy.

Whatever the result in 2033, it is likely that the UK will be still a leading player, both in research and in producing innovative companies like ORCA Computing.

14.IBM Cuts Through the Noise. What's the Potential Impact?

by David Shaw
https://quantumcomputingreport.com/ibm-cuts-through-the-noise-whats-the-potential-impact/

IBM have used their Eagle R3 processor to demonstrate effective execution of a 127Q circuit out to a gate depth of 60. Published in Nature, the result shows how the quantum device exceeds the capability of the best currently available classical alternatives. Furthermore it does this in a type of problem (the time evolution of a 2D transverse-field Ising model) that will impress many scientists as a pointer to future material science applications. IBM doesn't claim that this is quantum supremacy or quantum advantage in the terms often previously discussed. Side stepping a debate about possible future improvements in conventional algorithms or the definition of exponential quantum advantage, it has chosen to demonstrate an impressive practical capability in a problem suggestive of real world applications.

While the quantum community will welcome this new success, GQI believes that this is also a potential source of disruption within the sector.

The 100×100 will set new table stakes

IBM's result is a powerful indicator that it is on track to deliver its 100×100 challenge. This promises, by the end of 2024, the ability to consistently calculate expectation values from a 100Q by 100 gate depth circuit within a 24 hour run. IBM is already at 127×60 and Eagle R3 hasn't yet even benefited from the boost in 2Q gate fidelity we expect to see from the move to the tunable coupler architecture (pioneered in Falcon R10/Egret). we expect to see in its Heron devices.

100×100 is not a slam dunk for any specific known application, but it would clearly be a very interesting 'beyond classical' capability. We've been experiencing a halcyon era in quantum computing, where many different qubit vendors have competed to secure early hardware implementations around the world. Mostly this has supported research interest that wants to experiment on real devices, but that realizes that real code development might as well proceed on simulators anyway. Successful delivery of the 100×100 challenge promises to change that. Labs and facilities not able to offer their developers access to this new capability will increasingly feel removed from the cutting edge.

Algorithm developers will need to recalibrate

IBMs new route to useful NISQ era applications may also disrupt algorithm developers. The 100×100 challenge isn't just about improved hardware fidelity. It will require cutting edge error suppression. It also utilizes aggressive error mitigation. Techniques such as zero noise extrapolation and probabilistic error cancellation depend on a runtime regime that automatically iterates across a very high number of shots (hence the 24 hour clock time window).

GQI suspects that it's not going to be as straightforward as picking up existing VQA concepts and simply applying them to the new capability. Software players focussed on error suppression and error mitigation will do well as others play catchup. Quality will out as others seek to adapt to the new opportunities presented.

Significant NISQ revenues will mean pressure for those without

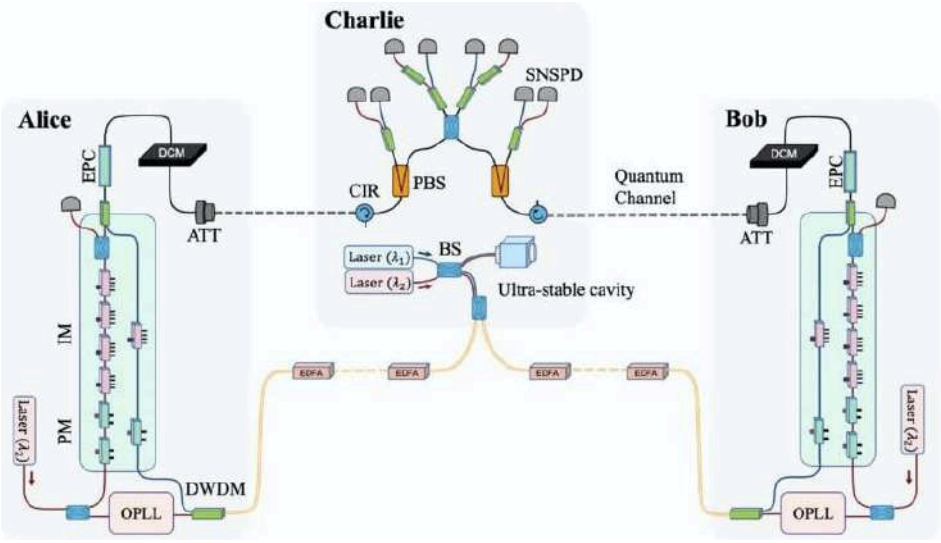
IBM has shown great progress, but it doesn't directly unlock its longer-term path to fault tolerant quantum computing (FTQC). Its architecture still faces the challenges of demonstrating the step-up in performance on thermal budget and interconnects that will require. However, even those competitors focussed on their own longer term roadmaps to fault tolerance will feel pressure from this announcement. Many have favored the view that commercial applications in the NISQ era were increasingly unlikely. IBM have not proven that these will be achieved, but they have significantly moved the dial back in that direction. Players without the prospect of access to those revenues will inevitably feel more pressure than those that do.

15.Scientists achieve 1,000 km quantum key distribution

by University of Science and Technology of China
https://phys.org/news/2023-06-scientists-km-quantum-key.html

A point-to-point long-distance quantum key distribution (QKD) over a distance of 1,002 km has been achieved by scientists from the University of Science and Technology of China (USTC) of the Chinese Academy of Sciences (CAS), and their collaborators from Tsinghua University, Jinan Institute of Quantum Technology, and Shanghai Institute of Microsystem and Information Technology (SIMIT), CAS. This milestone not only sets a new world record for non-relay QKD but also provides a solution for high-speed intercity quantum communication. The results were published in *Physical Review Letters* on May 25th.

QKD is based on the principles of quantum mechanics and enables secure key distribution between two remote parties. When combined with the "one-time pad" encryption method, it can achieve the highestlevel of security for confidential communication. However, the distance of QKD has been limited by factors such as the channel loss and system noise.



The twin-field QKD (TF-QKD) using sending-or-not-sending (SNS) protocol was demonstrated in the ex-

periment, improving the relation between the key rate and channel transmittance from a linear η to its square root η. Therefore, it can achieve a much longer secure distance than traditional QKD protocols.

To achieve long-distance QKD, the research team collaborated with Yangtze Optical Fiber and Cable Joint Stock Limited Company (YOFC) and used ultra-low-loss fiber based on pure silica core technology, which achieved a maximum attenuation of 0.16 dB/km. SIMIT developed ultra-low-noise superconducting single-photon detectors.

By implementing multiple filters at temperatures of 40 K and 2.2 K to suppress dark counts caused by thermal radiation, the noise of the single-photon detectors was reduced to around 0.02 cps. Furthermore, the team also developed a dual-band phase estimation scheme to avoid the spontaneous Raman scattering noise, reducing the system noise to below 0.01 Hz.

Based on the aforementioned technological developments, the team achieved TF-QKD over a record distance of 1,002 km, with a key rate of 0.0034 bps. This work not only verifies the feasibility of the SNS-TF-QKD scheme at extremely long distances but also demonstrates that this protocol can achieve high key rates in many practical scenarios.

The success of this study holds significant implications for the advancement of secure quantum communication. It opens up new possibilities for long-distance quantum key distribution and paves the way for the realization of high-speed intercity quantum communication networks.

16.Hackers can steal cryptographic keys by video-recording power LEDs 60 feet away

by Dan Goodin
https://arstechnica.com/information-technology/2023/06/hackers-can-steal-cryptographic-keys-by-video-recording-connected-power-leds-60-feet-away/

Researchers have devised a novel attack that recovers the secret encryption keys stored in smart cards and smartphones by using cameras in iPhones or commercial surveillance systems to video record power LEDs that show when the card reader or smartphone is turned on.

The attacks enable a new way to exploit two previously disclosed side channels, a class of attack that measures physical effects that leak from a device as it performs a cryptographic operation. By carefully monitoring characteristics such as power consumption, sound, electromagnetic emissions, or the amount of time it takes for an operation to occur, attackers can assemble enough information to recover secret keys that underpin the security and confidentiality of a cryptographic algorithm.

Side-channel exploitation made simple

As Wired reported in 2008, one of the oldest known side channels was in a top-secret encrypted teletype terminal that the US Army and Navy used during World War II to transmit communications that couldn't be read by German and Japanese spies. To the surprise of the Bell Labs engineers who designed the terminal, it caused readings from a nearby oscilloscope each time an encrypted letter was entered. While the encryption algorithm in the device was sound, the electromagnetic emissions emanat-

ing from the device were enough to provide a side channel that leaked the secret key.

Side channels have been a fact of life ever since, with new ones being found regularly. The recently discovered side channels tracked as Minerva and Hertzbleed came to light in 2019 and 2022, respectively. Minerva was able to recover the 256-bit secret key of a US-government-approved smart card by measuring timing patterns in a cryptographic process known as scalar multiplication. Hertzbleed allowed an attacker to recover the private key used by the post-quantum SIKE cryptographic algorithm by measuring the power consumption of the Intel or AMD CPU performing certain operations. Given the use of time measurement in one and power measurement in the other, Minerva is known as a timing side channel, and Hertzbleed can be considered a power side channel.

On Tuesday, academic researchers unveiled new research demonstrating attacks that provide a novel way to exploit these types of side channels. The first attack uses an Internet-connected surveillance camera to take a high-speed video of the power LED on a smart card reader—or of an attached peripheral device—during cryptographic operations. This technique allowed the researchers to pull a 256-bit ECDSA key off the same government-approved smart card used in Minerva. The other allowed the researchers to recover the private SIKE key of a Samsung Galaxy S8 phone by training the camera of an iPhone 13 on the power LED of a USB speaker connected to the handset, in a similar way to how Hertzbleed pulled SIKE keys off Intel and AMD CPUs.

Power LEDs are designed to indicate when a device is turned on. They typically cast a blue or violet light that varies in brightness and color depending on the power consumption of the device they are connected to.

There are limitations to both attacks that make them unfeasible in many (but not all) real-world scenarios (more on that later). Despite this, the published research is groundbreaking because it provides an entirely new way to facilitate side-channel attacks. Not only that, but the new method removes the biggest barrier holding back previously existing methods from exploiting side channels: the need to have instruments such as an oscilloscope, electric probes, or other objects touching or being in proximity to the device being attacked.

In Minerva's case, the device hosting the smart card reader had to be compromised for researchers to collect precise-enough measurements. Hertzbleed, by contrast, didn't rely on a compromised device but instead took 18 days of constant interaction with the vulnerable device to recover the private SIKE key. To attack many other side channels, such as the one in the World War II encrypted teletype terminal, attackers must have specialized and often expensive instruments attached or near the targeted device.

The video-based attacks presented on Tuesday reduce or completely eliminate such requirements. All that's required to steal the private key stored on the smart card is an Internet-connected surveillance camera that can be as far as 62 feet away from the targeted reader. The side-channel attack on the Samsung Galaxy handset can be performed by an iPhone 13 camera that's already present in the same room.

"One of the most significant things of this paper is the fact that you don't need to connect the probe, connect a scope, or use a software-defined radio," Ben Nassi, the lead researcher of the attack, said in an interview. "It's not intrusive, and you can use common or popular devices such as a smartphone in order to apply the attack. For the case of the Internet-connected video camera, you don't even need to approach the physical scene in order to apply the attack, which is something you cannot do with a software-defined radio or with connecting probes or things like this."

The technique has another benefit over more traditional side-channel attacks: precision and accuracy. Attacks such as Minerva and Hertzbleed leak information through networks, which introduces latency and adds noise that must be compensated for by collecting data from large numbers of operations. This limitation is what causes the Minerva attack to require a targeted device to be compromised and the

Hertzbleed attack to take 18 days.

Rocking the rolling shutter

To many people's surprise, a standard video camera recording a power LED provides a means of data collection that is much more efficient for measuring information leaking through a side channel. When a CPU performs different cryptographic operations, a targeted device consumes varying amounts of power. The variations cause changes in brightness and sometimes colors of the power LEDs of the device or of peripherals connected to the device.

To capture the LED variations in sufficient detail, the researchers activate the rolling shutter available in newer cameras. Rolling shutter is a form of image capture akin in someways to time-lapse photography. It rapidly records a frame line by line in a vertical, horizontal, or rotational fashion. Traditionally, a camera could only take pictures or videos at the speed of its frame rate, which maxed out at 60 to 120 frames per second.

Activating a rolling shutter can upsample the sampling rate to collect roughly 60,000 measurements per second. By completely filling a frame with the power LED that's presently on or connected to a device while it performs cryptographic operations, the researchers exploited the rolling shutter, making it possible for an attacker to collect enough detail to deduce the secret key stored on a smart card, phone, or other device.

"This is possible because the intensity/brightness of the device's power LED correlates with its power consumption, due to the fact that in many devices, the power LED is connected directly to the power line of the electrical circuit which lacks effective means (e.g., filters, voltage stabilizers) of decoupling the correlation," the researchers wrote in Tuesday's paper.

17.Post-Quantum: The New '2000 Effect'?

by Ayhan
https://www.natescrest.com/post-quantum-the-new-2000-effect-technology/

Avoided tragedies are deeply toxic because they make us believe we are immortal, untouchable, made of titanium, and make us distrust the doomsayers and Cassandras who tell us of doom and gloom. In tech it's called the "2000 effect," a story old people tell around motherboards as a big problem that never happened. As Sophia Petrillo says, it was New Year's Eve 199…

Avoided tragedies are deeply toxic because they make us believe we are immortal, untouchable, made of titanium, and make us distrust the doomsayers and Cassandras who tell us of doom and gloom. In tech it's called the "2000 effect," a story old people tell around motherboards as a big problem that never happened. As Sophia Petrillo says, it was New Year's Eve 1999. The world was on edge. The threat of the "Year 2000 effect" is real, and no one can accurately determine the impact this failure will have on the prehistoric technology of the time. The "Millennium Error" is based on the idea that no one will arrive by the year 2000 or, if they do, we'll already teleport away. *Star Trek* to another distant galaxy. We don't "future-proof" computers and computers don't keep years with four digits, but with two. So the risk of them changing from 1999 to 1990 when changing the year was real. But it didn't happen. Not because of a magical act, or because computers healed themselves, or because the doomsayers were wrong, but because many people prepared, worked hard, and avoided disaster.

The rest of us humans, oblivious to the effort, created a meme called the "2000 Effect" and went about our lives laughing at the absent wolf. Every time one wants to prevent a technology problem, one is al-

ways ready to remember the year 2000 or the last time money was spent on a remote failed technology project. The brothers-in-law give their opinion and many important things like security, they find reasons not to confront the madman by using their dull speech and using their cowardice wisely. These creatures we all know create so that nothing changes, so that in the medium term everything gets worse.

Right now we are in the middle of an experiment in the application of shock theory by artificial intelligence companies, however, we are not applying the precautionary principles we should have learned from that experience to other existential risk technologies. Like AIs at the time, quantum computers are one of those rare risks with an immature, expensive, difficult-to-operate and incomprehensible technology that no one can set a timeline for. I still remember the jokes about the results of generative AIs and the vague sayings that the incomprehensible, opaque and very expensive gadgets couldn't do anything useful for anyone. It seemed like it would never come, indicating the agenda that it was an unwanted visitor who came unexpectedly and wanted to stay and live.

In the quantum case, added is the complexity of quantum mechanics, an elusive branch of physics that is closer to mathematical belief than experience. In this paper Raoul Liman is devoting very interesting parts to quantum, in which he explains the edges of this theory that are used to practice better than I can do on this platform. In this regard, I limit myself to sharing the bewilderment of US President Joe Biden during his acceptance speech when he visited the IBM headquarters in Poughkeepsie and showed off a quantum computer. Chips and the Law of Science. Biden's face is a poem. We didn't realize that that chandelier hanging from an outdated theater would be capable of breaking a missile system's cryptography, all of our communications, or dissolving the blockchain like a sugar cube. I am sorry for the dissatisfaction *Cryptocurrencies* But if there is a quantum tsunami effect, we truly know what the existential risk is. Because if the encryption used for the data and systems of all states, companies and institutions collapses, their services collapse, and with them, society as we know it. It won't be an epidemic with Netflix and TikTok challenges. There will be a blackout where basic services will not be available for a limited period of time. The problem is that no one knows when it will happen, everyone knows how to prepare, but no one knows how. We don't know if it'll be around five or ten years from now, whether it'll work with the Visigothic crown that Biden is thinking about, or come up with some other lighter, simpler, and faster-to-use gadget. If it's the Chinese or the Americans. But there is consensus that it will happen. Like self-fulfilling prophecies, the more you believe the technology will work, the more you invest in making it work.

A practical problem arising from the theory that a quantum computer is capable of solving a mathematical problem in seconds now takes years to solve. We must defend ourselves against technology that threatens us. Meanwhile, governments such as the United States through the National Institute of Standards and Technology (NIST), which takes several years Dedicating efforts to the development of post-quantum cryptography This is because they rightly fear that building large-scale quantum computers could undermine many of the public-key cryptosystems that underpin the security and integrity of communications and information on the Internet. While both NIST and the US government believe it will take 15 to 20 years to get quantum computers, they don't think it's wise to wait until everything explodes. For this reason, the US federal government's Office of Management and Budget (OMB) has asked all federal agencies to identify the systems under their control. And, once identified, they plan to implement hybrid solutions (current and post-quantum encryption) for what might happen.

In short, we know something needs to be done, there are people doing it, but we don't know if it's going to work in the real world. It's in that critical period, between working quantum machines and seeing if countermeasures work, that we can kill ourselves as a society.

18.How the U.S. National Quantum Initiative Act Might Change When It is Renewed

by Ayhan
https://www.natescrest.com/post-quantum-the-new-2000-effect-technology/

The current U.S. National Quantum Initiative Act (QIA) was signed into law in December 2018 with authorized funding of $1.275 billion to be allocated to the National Institute of Standards and Technology (NIST), Department of Energy (DOE), and the National Science Foundation (NSF) to advance research into Quantum Information Science as well is provide funding for workforce development. In August 2022, the QIA was amended to include an additional $500 million for the DOE to establish a Quantum Network Infrastructure Research and Development Program and also an additional $165 million for the DOE to establish a `Quantum User Expansion for Science and Technology` (QUEST) program The concern in 2018 as it is today is for the United States to retain leadership in this technology, a concern which is equally shared on both sides of the political aisle.

The funding included in the original 2018 act only continues to the end of the 2023 Fiscal Year on September 30, 2023 and the U.S. Congress is now looking at renewing this act for 5 years or more. But it is clear to us that there will likely be changes in the budget allocations as well as the areas of focus. In 2018, the focus was on Science First which placed first priority on fundamental research. That was appropriate at the time, but now five years later the technology and the market has changed so we expect to see some changes. In this article, we will point out some of the changes in the Act that might occur in the next revision based upon the report from the National Quantum Initiative Advisory Committee as well as recent testimony to the House Committee on Science, Space, and Technology from five quantum experts. The expected changes will reflect the fact that the overall quantum ecosystem and level of international competition is different now than it was five years ago.

One concept for many of the potential changes listed below is a heavier focus on applications and commercialization rather than pure research. So here is our listing of a few potential changes we have heard proposed for when the act is renewed. This is only a partial list as it is likely there will be other suggestions that we haven't seen yet.

1. **Broaden government agency participation, particularly for those agencies that could be users of the technology**.
   The original QIA provided funding to the NSF, NIST, and DOE. Additional agencies that have increase interest in quantum technology could include the National Institute of Health (NIH), National Aeronautics and Space Administration (NASA), Department of Homeland Security (DHS), and the Department of Defense (DOD). While some of these agencies received quantum research funding from other programs outside of the QIA, there may be some merit to include specific funding for them in the QIA renewal.

2. **Encourage public/private partnerships to help accelerate the fruits of quantum research to bring these innovations to market.**
   One example, is a new directorate from the NSF called the Directorate for Technology, Innovation and Partnerships (TIP). Another example would be for funding an enhanced QUEST program to broaden user access to quantum resources for training and application development purposes.

Such program can benefit end users and quantum workforce development by allowing them access quantum computing resources that might not be affordable without this support. It also benefits providers by helping them obtain an enhanced revenue stream for supporting their quantum operations.

3. **Expand support for the additional types of workforce development programs.**
   Although the 2018 QIA did include funding for developing a quantum workforce. Much of the focus at that time was to support graduate level students seeking fellowships or postdocs to perform quantum research. Since then, a number of additional ideas for developing the quantum workforce have sprung up including programs for supporting mid-career engineers and programmers who want to move into quantum, early education to start teaching quantum concepts to high school and junior high school students, additional support for teaching quantum material undergraduate students, and bridge programs for students graduating with bachelors degrees to prepare them for graduate programs in quantum technology.

4. **Provide funding for improving the supply chain for quantum materials and components**
   In 2018, the availability of a robust quantum supply chain was not a great concern. Most of the activity was low volume R&D and there were more fundamental problems that needed to be solved then. Now, there are much greater concerns due to the larger volume requirements of basic raw materials and components, potential sourcing that may rely on unfriendly countries, a limited capacity and supplier choice to meet the demand. There was little or no funding in the 2018 QIA act to work on this issue, but it is an issue that organizations are now facing on a daily basis. For example, a material such as Helium-3 is a critical material for use in dilution refrigerators that has very limited sources. Some items such as dilution refrigerators or specialty lasers may have lead times that can last multiple months or even as long as a year or two. Other components may be single sourced and this poses a large risk if something happens to that one supplier.

5. **Increase support for cooperative partnerships with U.S. allies and leverage resources in other countries**
   Quantum technology is a difficult technology and to succeed the U.S. will need to work with friendly allies to help innovate, advance the technology, and to leverage the talent available in other countries. To that end, the United States has signed within the past few years several Statements of Cooperation in quantum technologies with countries including The Netherlands, France, Denmark, United Kingdom, Australia, Sweden, Finland, Switzerland, Japan, and others. Although these statements are nice as position statements we haven't seen any specific funding to back them up. The 2018 QIA did not include funding for supporting these types of programs. In recent years, many of these countries have budgeted significant amounts to fund their own internal programs and are much more advanced in quantum technology than they were five years ago. In addition, U.S. organizations would like to leverage foreign talent by increase various exchange programs, making it easier to get visa's and expediting immigration applications.

As the U.S. Congress considers how to renew the bill, they have a key concern. They very much want to maintain U.S. leadership while ensuring that U.S. quantum technology does not fall into the wrong hands of unfriendly actors. It will be a balancing act as to stringent export controls may impair the advancement of the technology, but controls that are too loose would be harmful to the U.S. interest too.

In the testimony we have seen so far, we have not yet heard anyone express a specific number with regards to the funding level. Whether the $1.275 billion funding in the 2018 QIA will be increased, decreased, or stay the same is not yet known. Under the recently passed debt ceiling bill, the U.S. non-defense spending will remain essentially flat for Fiscal 2024 and 2025 and possibly beyond. So any increases in the quantum funding levels may need to be taken at the expense of some other line item in the government's budget. So we can't make any predictions at this point about the absolute funding level, but we are certain that there will be differences in both the focus and how the funds are allocated towards the different programs and departments. However, the good news is that of all the issues facing

the U.S. government, support for advancing U.S. quantum technology is heavily supported by both political parties, so we are very certain that a renewal of the Quantum Initiative Act in some form will surely occur.

19.The Cryptography Arms Race: Governments, Hackers, and the Battle for Privacy

https://citylife.capetown/uncategorized/the-cryptography-arms-race-governments-hackers-and-the-battle-for-privacy/69560/

In today's digital age, the importance of privacy and security cannot be overstated. As our lives become increasingly intertwined with technology, the need to protect our personal information from prying eyes has become paramount. One of the primary methods of ensuring this privacy is through the use of cryptography, the science of encoding and decoding messages to protect their contents. However, as governments and hackers alike seek to gain access to our most sensitive data, a new arms race has emerged, with both sides vying for supremacy in the world of cryptography.

Cryptography has been used for centuries to protect sensitive information, with early examples dating back to ancient civilizations such as Egypt and Rome. However, the advent of the digital age has brought about a new era in cryptography, with increasingly complex algorithms and encryption methods being developed to protect our data. As technology continues to advance, so too does the sophistication of these cryptographic techniques, making it increasingly difficult for unauthorized parties to gain access to our personal information.

However, this has not stopped governments and hackers from attempting to break through these cryptographic barriers. In recent years, we have seen numerous examples of governments attempting to weaken encryption standards or gain access to encrypted data, often under the guise of national security. For instance, the United States government has been involved in a long-standing battle with technology companies such as Apple and Google over their use of strong encryption to protect user data. In 2016, the FBI famously sought to compel Apple to create a "backdoor" into the iPhone of one of the San Bernardino shooters, sparking a heated debate over the balance between privacy and security.

On the other side of the coin, hackers and cybercriminals are constantly seeking new ways to bypass encryption and gain access to sensitive data. This has led to the development of increasingly sophisticated hacking tools and techniques, as well as the rise of state-sponsored hacking groups that are often funded and supported by their respective governments. These groups are responsible for some of the most high-profile cyberattacks in recent memory, such as the WannaCry ransomware attack in 2017 and the SolarWinds hack in 2020.

As governments and hackers continue to wage war in the realm of cryptography, the battle for privacy has become increasingly complex. One of the primary challenges in this arms race is the concept of "quantum computing," a theoretical form of computing that could potentially break through even the most advanced encryption methods. While quantum computing is still in its infancy, the potential implications for privacy and security are immense, with many experts warning that it could render current encryption methods obsolete.

In response to these threats, researchers and technology companies are working tirelessly to develop new cryptographic techniques that can withstand the onslaught of government surveillance and hacking attempts. One such example is “post-quantum cryptography,” a field of study that seeks to develop encryption methods that are resistant to attacks from both classical and quantum computers. While these efforts are still in their early stages, they represent a crucial step forward in the ongoing battle for privacy.

Ultimately, the cryptography arms race between governments, hackers, and privacy advocates is a complex and ever-evolving struggle. As technology continues to advance and new threats emerge, the need for robust encryption and privacy protections will only become more critical. While the outcome of this battle remains uncertain, one thing is clear: the fight for privacy in the digital age is far from over.

20.Steps toward Southeast Asia’s first quantum-safe networks

by Muhammad Zulhusni
https://techwireasia.com/2023/06/singapore-southeast-asias-quantum-safe-networks/

The transition to quantum-safe networks requires careful planning and coordination. It involves evaluating the security vulnerabilities of existing systems, selecting suitable post-quantum algorithms, and updating network infrastructure and protocols.

Quantum computing is still in the early stages but organizations must proactively prepare for the post-quantum era by exploring quantum-safe solutions. Embracing quantum-safe networks enables them to future-proof their systems and ensure **long-term security** for sensitive data and communications.

During the **ATxSummit Social event**, part of Asia Tech x Singapore (ATxSG), Singapore’s deputy prime minister Heng Swee Keat unveiled the National Quantum-Safe Network Plus (NQSN+), an initiative aimed at establishing quantum-safe communications throughout Singapore and accelerating progress in the region.

The complexity of transitioning to quantum-safe networks

The launch of NQSN+ is a crucial element of Singapore’s Digital Connectivity Blueprint, introduced by Singapore’s minister for communications and information Josephine Teo, on June 5, 2023, prior to ATxSG. This blueprint outlines Singapore’s digital connectivity goals until 2030 and emphasizes the Infocomm Media Development Authority’s (IMDA) focus on enhancing the resilience and security of businesses in the digital economy through initiatives like NQSN+.

Quantum computers are poised to revolutionize various industries and drive innovation through unprecedented advancements in computing power, simulation, and optimization. However, the emergence of quantum computers brings security risks as they have the potential to break encryption algorithms relied upon today. Adopting quantum-safe technologies is crucial for safeguarding Singapore’s digital infrastructure and strengthening defenses against quantum attacks.

The National Quantum-Safe Network (NQSN), launched in 2022, serves as a vital foundation for Singapore’s journey toward quantum-safe networks. Building on more than a decade of quantum research by the Centre for Quantum Technologies (CQT), hosted by the National University of Singapore, NQSN conducted nationwide trials of quantum-safe communications technologies to enhance network security.

Collaborating with universities, companies, and government agencies, NQSN successfully demonstrated the technical feasibility of deploying quantum-safe technologies like Quantum Key Distribution (QKD). QKD protects against quantum computing risks by ensuring the secure transmission of keys, as any attempt to intercept them would disrupt the transmission and introduce errors.

The NQSN+ initiative enables critical information infrastructures such as hospitals and banks to utilize the quantum-safe system without the need to develop their own infrastructure. Additionally, the interoperability of telecommunications networks allows seamless communication for users, as stated by IMDA.

Securing Singapore's digital connectivity

During the Asia Tech x Singapore conference, Heng emphasized the importance of quantum technologies and highlighted Singapore's investment of over SG$250 million in quantum research since 2007.

As an initial step toward a quantum-safe Singapore, IMDA's NQSN+ initiative assists network operators in deploying nationwide quantum-safe networks. This facilitates businesses' access to solutions that protect their critical data. The implementation of NQSN+ involves a minimum of two network operators, each building an interconnected quantum-safe network capable of serving all businesses.

Organizations have the opportunity to collaborate with NQSN+ operators to integrate quantum-safe solutions and safeguard their vital data and information in the quantum age. IMDA is currently evaluating proposals from Singtel and a joint partnership between SPTel and SpeQtral.

Efforts to drive global standardization of quantum-safe technologies

Singapore actively collaborates with global leaders to promote interoperable quantum-safe networks. IMDA, in partnership with the NQSN team, leads global and local standardization efforts for quantum-safe technologies. In collaboration with Japan, Singapore co-leads the standardization of Quantum Key Distribution (QKD) protocols at the ITU Telecommunication Standardization Sector.

The joint effort aims to establish global standards for quantum-safe technologies. Singapore has already published its first Reference Specification on QKD Networks at the domestic level, providing guidance to technology vendors and organizations interested in deploying QKD networks.

International connectivity plays a vital role in Singapore's position in the global economy. Singapore aims to further strengthen its quantum initiatives by integrating the NQSN+ with quantum-safe networks in other cities. This will enable Singaporean enterprises to develop and deploy quantum-safe solutions across global markets.

As a preliminary step, IMDA has entered a memorandum of understanding with the National Information Society Agency of the Republic of Korea. This collaboration aims to foster cooperation in the field of quantum technologies and standardization efforts. The primary objective is to facilitate the exchange of knowledge and experience between network operators involved in the implementation of quantum-safe networks.

The journey toward quantum-safe networks is critical to securing Singapore's digital connectivity and ensuring resilience against emerging quantum threats. By taking proactive measures, Singapore is positioning itself as a leader in quantum technology adoption and paving the way for a quantum-safe future. The collaboration between IMDA, NQSN+, and various stakeholders demonstrates Singapore's commitment to driving innovation and safeguarding its digital infrastructure in the quantum age.

21.Chinese quantum computer is 180 million times faster on AI-related tasks, says team led by 'father of quantum' Pan Jianwei

by Holly Chik
https://www.scmp.com/news/china/science/article/3223364/chinese-quantum-computer-180-million-times-faster-ai-related-tasks-says-team-led-physicist-pan

Scientists in China say they have reached another milestone in quantum computing, declaring their device Jiuzhang can perform tasks commonly used in artificial intelligence 180 million times faster than the world's most powerful supercomputer.

The problems solved by their quantum computer could be applied to data mining, biological information, network analysis and chemical modelling research, the researchers said.

"Our work is a step toward testing real-world problems using the existing noisy intermediate-scale quantum computers," wrote the team headed by Pan Jianwei, a physicist at the University of Science and Technology of Chinawho has been dubbed the country's "father of quantum".

Their article was published in the peer-reviewed journal Physical Review Letters last month.

In the experiment, the team used Jiuzhang to solve a problem that is challenging for classical computers. It used more than 200,000 samples to solve the problem.

The researchers, for the first time, used the quantum computer to implement and accelerate two algorithms – **random search** and **simulated annealing** – that are commonly used in the field of AI.

The fastest classical supercomputer in the world would take 700 seconds for each sample, meaning it would take nearly five years to process the same number of samples.

It took Jiuzhang less than a second.

In a synopsis article published by Physics, a magazine from the American Physical Society that reports on papers from the Physical Review journals, the editor wrote: "the result extends the list of tasks for which today's noisy quantum computers offer an advantage over classical computers".

"Previous claims of quantum advantage were challenged by suggestions that the quantum computer was not competing against the best-possible classical algorithm for the task," the article said. "Whether the team's quantum processor will still yield an advantage over classical algorithms optimised for solving graph problems is an open question."

In traditional computing, a bit represents either zero or one as its basic unit of information. A qubit goes a step further. It can represent zero – one or both at the same time – one of the simplest expressions of the peculiarity of quantum mechanics.

Since the basic information of a quantum computer can represent all possibilities simultaneously, they are theoretically much faster and more powerful than the regular computers we use in our daily lives.

But the subatomic particles at the heart of the technology are fragile, short-lived and prone to error if exposed to even a slight disturbance from the surroundings. Most quantum computers operate in extremely cold and isolated environments to avoid disruption.

Jiuzhang, named after a 2,000-year-old Chinese maths text, uses light as the physical medium for calculation. Unlike other quantum computers, it does not need to work sealed in extremely low temperatures and can operate with stability for longer.

22.QuSecure Awarded U.S. Army Contract for Post-Quantum Cybersecurity Solutions

by Dan Spalding
https://www.businesswire.com/news/home/20230608005339/en/QuSecure-Awarded-U.S.-Army-Contract-for-Post-Quantum-Cybersecurity-Solutions

QuSecure™, Inc., a leader in post-quantum cybersecurity (PQC), today announced the United States Army has awarded the company a Small Business Innovation Research (SBIR) Phase II Federal Government contract to develop quantum-resilient software solutions.

With this award, QuSecure will continue to advance research and development of quantum-resilient technologies and encryption solutions for the U.S. Government. The award states that QuSecure's work has merit, will result in important benefits for the Army, and allots upwards of $2 million to address uses in tactical edge and tactical IoT devices that can be used for battle-ready deployment.

The U.S. Government's urgency to move toward a quantum safe future has been established with the recent actions taken by Congress and the White House. The Endless Frontiers Act establishes a Technology and Innovation Directorate at the National Science Foundation to use $100 billion in federal funds over five years to research emerging technologies including quantum computing, and specifically mentions the need for PQC. Additionally, in December 2022 President Biden signed into law the Quantum Computing Cybersecurity Preparedness Act, which requires the Office of Management and Budget to prioritize federal agencies' migration to IT systems using post-quantum cryptography.

"Following winning our U.S. Air Force SBIR Phase III award last Fall, QuSecure is proud to be a part of the Army's march toward a more cybersecure future," said Aaron Moore, QuSecure Head of Engineering, who also led R&D efforts for Defense Advanced Research Project Agency (DARPA). "This award from the Army recognizes QuSecure's ability to help enhance the combat fighting capabilities that modern warfare necessitates."

Last year the U.S. Government awarded QuSecure a U.S. Air Force SBIR Phase III Federal Government procurement contract for PQC solutions after executing a successful PQC pilot project deployed at a federal facility. QuSecure remains the industry's only PQC vendor earning the Phase III designation, establishing the company as the Federal Government's leading provider of PQC solutions, and setting the standard for all Federal Government's PQC requirements. With today's news on QuSecure's U.S. Army SBIR Phase II contract, QuSecure has further burnished its cybersecurity credentials with the U.S. military.

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

23.ISARA and The LightBridge Group Partner to Advance Post-Quantum Cryptography in Government

by ISARA
https://www.prnewswire.com/news-releases/isara-and-the-lightbridge-group-partner-to-advance-post-quantum-cryptography-in-government-301845084.html

ISARA, the leader in post-quantum cryptography (PQC) and cryptographic risk management, and The LightBridge Group, today announced their strategic partnership to advance post-quantum cryptography solutions and risk management services across the U.S. government.

"The LightBridge Group brings decades of government experience and insight which, in addition to its quantum science and cybersecurity expertise, complements ISARA's capabilities and roadmap plans. We warmly welcome this partnership and look forward to advancing PQC and cryptographic risk management, together, at the federal level," stated Atsushi Yamada, CEO of ISARA.

Quantum Computing Prioritization and Leadership at the Federal Level

U.S. President Joe Biden signed the Quantum Computing Cybersecurity Preparedness Act into law on December 21, 2022. The law sets requirements for federal agencies to inventory their active cryptographic assets, assess their vulnerabilities to future quantum computers, and perform proof-of-concept testing of post-quantum cryptographic algorithms.

"U.S. Government agencies are committed to preparing their IT systems for the arrival of cryptography-breaking quantum computers," said Jonah Force Hill, Managing Director & Head of Client Services at The LightBridge Group. "We believe that ISARA has the right experience and the right technologies to address the government's critical, quantum-safe needs."

Hill previously served as the director for cybersecurity and emerging technology on the staff of the National Security Council at The White House, where he was responsible for directing President Biden's National Security Memorandum on post-quantum cryptography (NSM 10).

24.The Need for a Comprehensive Strategy Addressing Cybersecurity and Quantum Technology

by Michael Brown
https://www.hstoday.us/featured/perspective-the-need-for-a-comprehensive-strategy-addressing-cybersecurity-and-quantum-technology/

Over the past two years, the Biden administration has taken a series of steps centered on quantum and cybersecurity. This has been done via a series of individual Executive Orders (EO), National Security Memorandums (NSM), ongoing technology research, development, test and evaluation, as well as other procurement and acquisition actions. The most recent presidential actions have focused on Quantum Information Science (QIS). These moves should be viewed together with the actions previously taken around cybersecurity and planned activities such as the forthcoming National Cybersecurity Strategy developed by the Office of the National Cyber Director. What is lacking, however, is a comprehensive view, i.e., strategy, for the federal government.

Mid-career officers in the Navy, along with the other Armed Services, are taught the operational art of joint warfighting and planning. I am not advocating war, but officers learn the value of planning and executing military operations via three lenses: strategic, operational, and tactical. All are very important when executed separately but having them linked together delivers enormous capability and capacity for whatever mission or operation is being planned. This approach is also very valuable outside the military domain – relevant in other federal, state, and local organizations, and absolutely applicable within the private sector. By using these processes, priorities and ideas combined with capabilities and capacities, also highlighting gaps, organizations can develop realistic plans to solve a specific problem.

Our problem today is a race to a secure ecosystem based on QIS with cybersecurity in place ahead of our strategic adversaries. We are well aware of both the threat and the overall activities that nation-states are executing in this realm. Several years ago, these adversaries adopted comprehensive strategies centered on modern technology and QIS to advance their internal economy, but also to use against us in myriad ways. China has put their strategy into practice over the past few years. They continue to plan and resource their multi-year efforts through an aggressive mix of intelligence/intellectual property theft combined with their own research and development.

We don't need to debate whether other nations are ahead of us with respect to QIS and cybersecurity. We know the threat is real and contributes to the need for action. But what the U.S. is missing is a comprehensive, integrated, prioritized strategy to address QIS and cybersecurity. We have the leadership in both the public and private sectors to put this strategy together. In addition, we have the technologies, the workforce, and indeed the resources to make it happen. In other words, we have the chef and we have the ingredients – we need the recipe!

As we review the actions from the past two years, there have been a lot of great operational and tactical activities. Some are connected while others are stovepipes addressing a certain issue. We have seen actions by both the Biden administration and Congress to highlight and address certain aspects of QIS and cybersecurity. That is great. However, a true strategy that comprehensively addresses QIS, cybersecurity, artificial intelligence, and other groundbreaking technologies is missing from our arsenal of capabilities. As mentioned, our adversaries have already adopted strategies and our national and economic

security rests upon our ability to quickly pull together the strengths from the public and private sectors. An example of a public-sector strength is the ability to bring organizations together and develop comprehensive planning. Likewise, a private-sector strength is the ability to innovate using technology, identify important use cases, and deploy them in critical infrastructure.

This has been done before and it is as important to state what the strategy is focused on as much as what it is not. In 2007, after nation-state cyberattacks and breaches targeting the public sector, President Bush signed the Comprehensive National Cybersecurity Initiative (CNCI). As the title states, it was a comprehensive approach from a strategic perspective to address role/responsibilities, technologies, and oversight for the federal government. It was not a comprehensive approach to the private sector's cybersecurity needs, though it depended on the expertise and capabilities from the private sector. This was a strategic approach to the issue, which led to the development of operational capabilities and plans within the federal government that were complemented with tactical actions focused on people, process and technology. By doing this, the government developed and defended a five-year plan which included resources (people and money) combined with legislative and executive actions to clarify roles and responsibilities. While not perfect, over the years this strategy has been adopted by the succeeding administrations and updated, expanded, and actions clarified within the federal government. It has also brought regulatory and best practices to the private sector.

When looking at President Biden's National Security Memorandums on Advancing Quantum Technologies and Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems, and his Executive Order on Improving the Nation's Cybersecurity, we see an attempt to take operational steps to meet the challenges of today and tomorrow. These are important – yet not strategic and not necessarily connected. Hopefully, the aforementioned National Cyber Strategy will indeed be strategic and the groundbreaking document necessary to develop comprehensive and integrated actions that can support the appropriate reallocation of resources, and potentially new resources, for the federal government over time. Here are a few ideas that this new strategy should include:

1. A clear thesis about the application of the strategy. It should include the technologies and ecosystem addressed and those necessary to achieve the results.

2. A clear description of the roles and responsibilities necessary to execute the strategy.

3. A clear outcome at the end of the strategy. The strategy should be used to define a clear plan of action and milestones (POA&M) that at the end of a certain time (perhaps 5 years) deliver the outcome we need.

4. The POA&M, based on the specifics within the strategy, will identify the roles and responsibilities required to execute the strategy. This will include the private sector as a critical partner in the development of the strategy and the follow-on execution.

5. A clear partnership between the Executive and Legislative branches. While the Executive Branch will author and execute the strategy, it will require partnership from the Legislative Branch for both proper authorities and resources.

While the strategy is critical for our national success, ongoing activities should continue, increase, and be linked together. NIST has been leading in the development and understanding of Post Quantum Cryptography. DoD and DHS are looking at the potential technologies to adapt and to develop use cases that would allow for quick action now. It is time for these and other efforts to be connected via one national strategy.

25.Post-Quantum Cryptography: Exploring the Future of Secure Communications

by André De Bonis
https://citylife.capetown/uncategorized/21st-century-technologies-post-quantum-cryptography/31294/

As we enter the third decade of the 21st century, the world is witnessing an unprecedented surge in technological advancements. Among these developments, quantum computing has emerged as a groundbreaking innovation that promises to revolutionize the way we process and transmit information. However, this new frontier of computing also poses significant challenges to the security of our digital communications. To address these concerns, researchers and industry experts are increasingly focusing on post-quantum cryptography, a field dedicated to developing cryptographic algorithms that can withstand the power of quantum computers.

Quantum computing is based on the principles of quantum mechanics, a branch of physics that deals with the behavior of matter and energy at the atomic and subatomic levels. Unlike classical computers, which use bits to represent information as either 0s or 1s, quantum computers use quantum bits, or qubits, which can represent both 0 and 1 simultaneously. This property, known as superposition, allows quantum computers to perform complex calculations at speeds that are orders of magnitude faster than their classical counterparts.

The rise of quantum computing has significant implications for the security of our digital communications. Most of the encryption schemes currently in use, such as RSA and elliptic curve cryptography, rely on the difficulty of factoring large numbers or solving discrete logarithm problems. While these problems are computationally infeasible for classical computers, they can be solved relatively quickly by quantum computers using Shor's algorithm. This means that once large-scale quantum computers become a reality, they could potentially break the encryption that protects our sensitive data, including financial transactions, personal communications, and national security secrets.

To counter this threat, researchers are developing post-quantum cryptographic algorithms that are believed to be resistant to quantum attacks. These algorithms are based on mathematical problems that are considered hard for both classical and quantum computers, such as lattice-based cryptography, code-based cryptography, and multivariate cryptography. In addition to these, hash-based signatures and isogeny-based cryptography are also being explored as potential post-quantum solutions.

One of the key challenges in developing post-quantum cryptography is striking a balance between security and efficiency. While some of the proposed algorithms offer strong resistance against quantum attacks, they often come with increased computational complexity and larger key sizes, which can result in slower encryption and decryption processes. Moreover, the lack of a standardized framework for evaluating the security of post-quantum algorithms makes it difficult to determine their true resilience against quantum threats.

Recognizing the importance of post-quantum cryptography, several organizations and governments have initiated efforts to standardize and promote its adoption. The National Institute of Standards and Technology (NIST) in the United States has been leading a global effort to develop a suite of standardized post-quantum cryptographic algorithms. The process, which began in 2016, has received submissions from researchers around the world and is currently in its third round of evaluation. NIST aims to finalize the selection of post-quantum algorithms by 2022, paving the way for their widespread implementation.

26.Data security via quantum computing

by Sean Duca
https://www.manilatimes.net/2023/06/04/business/sunday-business-it/data-security-via-quantum-computing/1894374

The Philippines is gearing up to advance its digital transformation. Bills such as the E-Governance Act, the Internet Transactions Act and tax reforms are being reviewed to accommodate digital service providers and foster an environment that would ease the adoption of emerging technologies.

As a result, businesses will be empowered to integrate technologies that contribute to higher economic growth and improve the quality of life for Filipinos. However, it is crucial to acknowledge that these tools could be detrimental if maliciously utilized.

Quantum computing is one of these technologies that organizations need to watch out for. By allowing the performance of multiple computations simultaneously, quantum computing is faster and more potent at processing massive amounts of data than classical computing. This feature is highly appreciated in practices such as health care, with the promise of a more comprehensive analysis of a patient or the discovery of a new drug for the incurable at unprecedented speed.

However, if taken from a cybersecurity context, the same capability creates unknown risks and exposures, particularly around its ability to break most modern encryption, which underpins the internet, communications and e-commerce — the very fabric of our society.

Decoding the math behind encryption

Encryption is the process of converting an original piece of human-readable information and transforming it into incomprehensible text using an encryption algorithm and cryptographic key. The two primary forms of encryption are symmetric, in which the same key is used to encrypt and decrypt the data, and asymmetric, which involves a pair of mathematically linked keys. Symmetric encryption is fast, efficient, and most widely used to secure communications and stored data.

Meanwhile, asymmetrical or public-key encryption is used to securely exchange symmetric keys and digitally authenticate certificates, messages, documents and e-commerce payments, pairing the public keys with their owners' identities. While the math is different, nearly all internet communications use symmetric and asymmetric cryptography. Hence, both forms need to be secure.

The threat of a data breach comes when cybercriminals potentially use quantum computing to manipulate probabilities and perform calculations at an unprecedented speed to find the values that would break public-key encryptions. A further danger is also seen with these perpetrators stealing data — intellectual property, financial, or health care information that could still be relevant beyond the next decade — to be decrypted later, or known as the "harvest now, decrypt later" (HNDL) attack.

A large-scale quantum computer could also decrypt the most common cybersecurity protocols and all previously recorded traffic, putting economic prosperity, national security and people's lives at risk.

Post-quantum data security posture

To prepare for the security threats of quantum computing, organizations could start by thinking about

post-quantum cryptography (PQC) algorithms and replacing current algorithms with new quantum-resistant algorithms. While PQC solutions are still in development, organizations should evaluate the security of post-quantum candidates and transition to using these algorithms to ensure their data remains secure.

Another option is quantum key distribution (QKD), creating a shared secret between users to create secure transmissible messages over conventional channels. It requires special-purpose technology, such as a high-quality optical fiber infrastructure. However, it is a method to protect session keys against being compromised.

Organizations must also consider updating their procurement policies, mandating that future technology purchases require cryptographic flexibility and scalability.

Realistically, quantum security should not be viewed as a replacement for existing measures, but as an additional form of security that must be managed alongside the current infrastructure. As a result, organizations must consider how they will deploy, manage, and maintain both conventional and post-quantum security on their systems.

Sean Duca is the vice president and regional chief security officer for Asia-Pacific & Japan at Palo Alto Networks, an American multinational cybersecurity company with headquarters in Santa Clara, California, whose core product is a platform that includes advanced firewalls and cloud-based security offerings.

27.In-Depth Report of Quantum Security and PQC Market Size

by Matt Swayne
https://thequantuminsider.com/2023/06/02/quantum-security-and-pqc-market-size/

Current communication protocols heavily rely on public key encryption, digital signatures and key exchange, but the ability of quantum computers to efficiently solve mathematical problems threaten these protocols, which, essentially, are running the world's economy.

The 2023 Quantum Security Report from **The Quantum Insider** offers readers a deep understanding of the quantum security market size and key players in the growing quantum security ecosystem that seeks solutions to security and privacy in what experts refer to as the post-quantum cryptography era.

The report shows that Post-Quantum Cryptography — or PQC — is gaining momentum as a way to create algorithms secure against decryption by quantum computers, leading to a rapidly growing funding environment and an expanding PQC market.

"Organizations — from government agencies to businesses to startups — are working to prepare us for the coming post-quantum security era," said Alex Challans, CEO of The Quantum Insider. "Timing is crucial for people concerned about PQC to get up to speed about the technology, the players and the range of outcomes of what is shaping up to be a historic global effort to ensure security and maintain privacy."

Some of the technologies and PQC approaches covered in the report:

- Quantum Random Number Generators (QRNGs)
- Post-Quantum Cryptography (PQC)
- Quantum Key Distribution (QKD)
- Quantum Communications & Quantum Internet

Mapping the Ecosystem

Quantum security is built with extremely complex technologies — and the ecosystem is just as complicated and complex. The report breaks this down with market segmentation and a comprehensive ecosystem map. The breakdown includes 120+ key companies by classification and geography and features "xtrip" profiles of these key players. There is also a breakdown and overview of major academic and national initiatives in the US and internationally.

Recent Efforts

The report also reviews the recent history of PQC actions including the National Institute of Standards and Technology's (NIST) efforts to address quantum security concerns by searching for a quantum-resistant algorithm to replace the RSA public key standard. It also reviews the rise of harvesting attacks. In these attacks, encrypted data is stored until a quantum computer can decrypt it, further emphasizes the urgency of quantum-resistant encryption.

The data in the report is sourced from sector experts, The Quantum Insider's market intelligence platform, utilizing public announcements and information from companies in the quantum security field.

28.WithSecure's USB armory enables post-quantum cryptography in space

https://www.helpnetsecurity.com/2023/06/01/withsecures-usb-armory-enables-post-quantum-cryptography-in-space/

WithSecure's USB armory is an open-sourced, single board computer with a unique form factor and capabilities. It has been used in a variety of applications, including (but not limited to) encrypted storage solutions, hardware security modules (HSM), enhanced smart cards, electronic vaults (e.g. cryptocurrency wallets), key escrow services, and more.

MAPHEUS, or Material Physics Experiments in Zero Gravity, is a program operated by the German Aerospace Center's (DLR) Materials Physics in Space and Aerospace Medicine institutes, and the Mobile Rocket Base (MORABA).

Their latest mission, MAPHEUS-13, was launched on May 22, 2023, to conduct experiments on 3D printing components made of metal in zero gravity, the response of molten alloys to weightlessness, healing processes in the central nervous system or brain in reduced/increased gravity, and more.

Included in the mission as a part of Experiment 007 EV2 was WithSecure's USB armory to assess its security framework and capabilities for protecting data produced by experiments. Specifically, it aimed to assess post-quantum cryptography for secure key exchange in a trusted execution environment running on a USB armory.

"We were looking for a solution to extend our real-time systems in Experiment 007 with a secure computer system that allows us to integrate computing power for more advanced algorithms, data analysis, and standard software in a neat, lean, and secure way. The USB armory proved to be small, versatile, and powerful enough to fit our requirements. In the long run we will extend the use of TamaGo, GoTEE and Linux to enable complex data analysis and AI/ML use-cases for the scientists at DLR in-flight," said DLR partner and Chief Security Architect at adesso SE Christian Kahlo.

The USB armory's versatility and entrenched security features have provided a suitable base for additional security frameworks. These include TamaGo, which reduces attack surfaces by removing dependency on memory-unsafe languages, operating systems, and third-party libraries; and GoTEE, a trusted execution environment that allows the device to isolate secure applets from unsafe code, with and without operating systems.

Thanks to this combination of capabilities, the USB armory successfully exchanged encryption keys using post-quantum cryptography during the mission.

"This is the first time we put the USB armory into space. I'm pleased that our hardware and software did its job in this environment. We enabled advanced cryptography in space, and on top of this, we did it with memory safe code and a minimal software supply chain thanks to our TamaGo and GoTEE frameworks. Our team is extremely proud of this collaboration and its accomplishments," said WithSecure Head of Hardware Security Andrea Barisani.

29.Congressional Hearing to Gauge U.S.'s Commitment to National Quantum Initiative

by Matt Swayne
https://thequantuminsider.com/2023/06/01/congressional-hearing-to-gauge-u-s-s-commitment-to-national-quantum-initiative/

The U.S. Congress will schedule a hearing on the advancement of quantum technologies on June 7, according to the House Committee on Space, Science and Technology website. Funding the country's National Quantum Initiative — NQI — into the future may be one of the subjects up for debate.

The committee is chaired by Frank Lucas and the session will likely include testimony from witnesses Paul Dabbar, former Undersecretary for Science, Department of Energy; Eleanor G. Rieffel, Chief Scientist, NASA Ames; Celia Merzbacher, Executive Director, Quantum Economic Development Consortium and Emily Edwards, Executive Director, IQUIST, University of Illinois.

Dabbar, who is currently the CEO of quantum communication startup Bohr Quantum, writes in a LinkedIn post that this may be an ARPA-Net-like moment, with quantum technologies maturing swiftly and a unique commercial-academic ecosystem emerging just as fast.

He writes: "Today Congress is looking at reauthorizing NQI for another five years. Quantum computing is now close enough to start looking at U.S. Department of Energy (DOE) Natl Labs to stand up a next supercomputer design and purchase cycle including QPU's in an architecture. And the technology is there

for first natl deployments of quantum networks – leading to the quantum internet, just like ARPA-Net in 1969 triggered NSF Net and ultimately the Internet."

With national security issues in the mix and a stiffening block of competitiveness in the field, there's little to suggest that Congress will walk away from NQI. In fact, it may be strengthened. NQI had broad bi-partisan support at a time when bi-partisanship is rare.

Dabbar, who was part of the passing of the legislation as undersecretary, believes that the program's initial success as a catalyst for quantum should warrant an extension.

Dabbar writes: "The significant increase in quantum tech not only stood up large new efforts at National Labs and universities, it also triggered the private sector to invest over $6 billion in the area. In the investing community we call that "leverage". I like to call the US government funding of the NQI "seed capital". And a series of tech accomplishments resulted from that."

30.Post-Quantum Cryptography: The Algorithms That Will Protect Data in The Quantum Era

by Bart Stevens
https://semiengineering.com/post-quantum-cryptography-the-algorithms-that-will-protect-data-in-the-quantum-era/

There is no doubt that quantum computers will play a significant role in helping the world solve complex challenges not possible on current classical computers. However, quantum computers also pose a serious security threat. They will eventually become powerful enough to break traditional asymmetric cryptographic methods, that is, some of the most common security protocols used to protect sensitive electronic data including your bank account and medical records. Even data that is stored and considered secure today will be at risk in the quantum era.

Once sufficiently powerful quantum computers exist, traditional asymmetric cryptographic methods for key exchange and digital signatures will be easily broken. Leveraging Shor's algorithm, they will reduce the security of integer discrete logarithms like Elliptic Curve Cryptography (ECC) and RSA (Rivest-Shamir-Adleman) so much that no reasonable key size would suffice to keep data secure. Conversely, symmetric cryptography in general, and Advanced Encryption Standard (AES), Secure Hash Algorithm 2 (SHA-2), and SHA-3 in particular, are expected to suffer a much smaller security reduction from quantum computers; using large key sizes will be enough.

Governments, researchers, and tech leaders the world over have recognized this security threat and the associated challenge to secure critical infrastructure against quantum computers. Many initiatives have been launched to develop and deploy new cryptographic algorithms that can replace RSA and ECC without being vulnerable to either classic or quantum attacks. This is what is commonly referred to as "Post-Quantum Cryptography" (PQC), "Quantum Safe," "Quantum Proof" or "Quantum Resistant" cryptography.

The biggest public initiative to develop and standardize new PQC algorithms was launched by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). After six years of

competition, in July 2022 NIST announced the first group of algorithms designed to withstand a quantum attack. The four encryption algorithms selected will become part of NIST's post-quantum cryptographic standard, expected to be finalized in the coming years. CRYSTALS-Kyber was selected as a Key Encapsulation Mechanism (KEM) and CRYSTALS-Dilithium, FALCON, and SPHINCS+ were selected as digital signature algorithms.

Following NIST's algorithm selection, in September 2022, the National Security Agency (NSA) published an update to its Commercial National Security Algorithm Suite (CNSA). CNSA 2.0 specifies that CRYSTALS-Kyber and CRYSTALS-Dilithium should be used as quantum-resistant algorithms. In addition to these, the stateful hash-based signature schemes XMSS (eXtended Merkle Signature Scheme) or LMS (Leighton-Micali Signatures) are to be used for firmware protection. The update provides an ambitious migration timeline for the US government and its suppliers to adopt these new PQC algorithms. The NSA requires all National Security Systems (NSS) to fully transition to PQC algorithms by 2033, with some use cases required to complete that transition as early as 2030.

Other organizations throughout the world have also published their own guidelines on PQC. The common theme in Europe is that the NIST algorithm selection is good, but that Frodo KEM and Classic McEliece KEM algorithms are also acceptable. For use cases where KEMs must be chosen with a focus on long-term security, these may be favored by some European governments. Clear timelines for standardization of additional algorithms or migration projects are still a work in progress. It is possible that in the coming years we may see the standardization of additional PQC algorithms happen within international organizations, such as the Internet Research Task Force's (IRTF) Crypto Forum Research Group or the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC).

Quantum computing is being pursued across industry, government and academia with tremendous energy and is set to become a reality in the not-so-distant future. For many years, Rambus has been a leading voice in the PQC movement and continues to develop algorithms and products designed to secure our customers' data and devices. Solutions like the Rambus Root of Trust portfolio anchor security in hardware, include AES and SHA cryptographic cores, and offer programmability to incorporate new functionality to futureproof designs.

