Crypto News

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

November 01, 2023

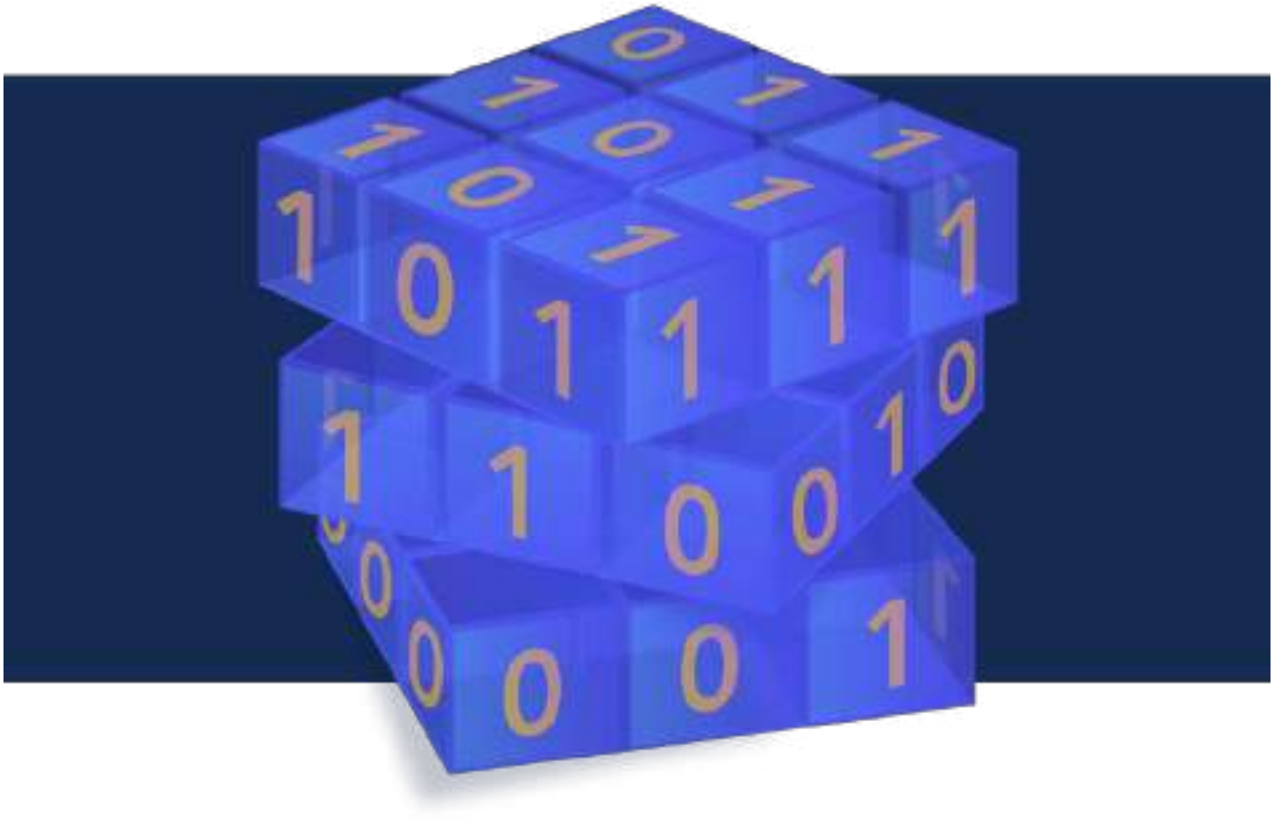

TABLE OF CONTENTS

Editorial

With the explosion in the number of posts/articles/comments related to Quantum/Post-Quantum/Quantum-Safe and similar, it is hard to keep track. This compilation of Crypto News from Dhananjoy is a great way to start. In a compact format, you can have a first glimpse of the 25 selected pieces, then go deeper into what you find most interesting.

On my side, this month I have selected number 14: STANDARDS BODY CONSIDERS UNCLOAKING SECRET ENCRYPTION ALGORITHMS. I have to admit that I was not aware that the European Telecommunication Standards Institute (ETSI) had standardised a suite of secret algorithms for the encryption of radio communications, the TETRA, which is used by police, the military and critical infrastructures among others. This secrecy prevented independent security experts to investigate possible vulnerabilities. And guess what? A group of Dutch researchers managed to reverse-engineer a radio they purchased, extract the algorithms, and found flaws and even a backdoor. We can only hope that the bad guys were not as clever…

This is a textbook example of what you should NOT do in cryptography. In all my presentations, I mention Kerckhoff's principle, which states that the security of a cryptosystem should only depend on the keys. All the rest, including the algorithms should be considered public. The ETSI seems to have forgotten this basic principle. Or maybe they have never followed one of my presentations…

At least, it seems that NIST is not following the same approach in their choice of the new post-quantum algorithms. The algorithms are truly in the public domain. And there are heated discussions between the experts investigating them. You can actually follow this on the post-quantum cryptography forum (https://lnkd.in/e7ngfwdu).

So kudos to NIST for at least trying to be transparent. And remember: any crypto system, which is kept secret should be treated carefully…

Many other pieces are really interesting this month. Choose well and have a good read!

The Crypto News editorial is authored by the Chair of the Quantum-Safe Security Working Group (QSS WG) of the Cloud Security Alliance (CSA), Bruno Huttner, Director of Strategic Quantum Initiatives at ID Quantique SA 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.NATO eyes ‘quantum-resistant’ encryption in 5G drill

by Elisabeth Gosselin-Malo
https://www.defensenews.com/home/2023/10/31/nato-eyes-quantum-resistant-encryption-in-5g-drill/

NATO member countries have set their sights on securing military 5G communication networks against hacking by adversaries possessing powerful quantum computers.

Alliance officials hosted an exercise to that effect earlier this month at a test site in Latvia. The event, dubbed 2023 Next-Generation Communication Network Technologies, was organized by NATO’s Allied Command Transformation and the Latvian defense ministry to present systems capable of enabling multi-domain operations. The term refers to the seamless coordination of land, air, naval, space and cyberspace assets in military campaigns.

One of the focus areas was for demonstrators to showcase approaches to improve command-and control-capabilities with the use of virtual reality, secure post-quantum encryption and apply sensor fusion for situation awareness, according to a press release provided by the organizers.

Scientists have warned for some time of the threat posed by quantum computers to crack common encryption algorithms that protect military hardware and intelligence operations.

The sense of urgency has ushered in the term “quantum-resistant encryption” to describe next-level security mechanics.

Last September, the U.S. National Security Agency (NSA) released the future quantum-resistant algorithm requirements for national security systems. Considering ongoing pursuits in quantum computing by international actors, the report called on industry “to now plan, prepare and budget for a transition.”

NATO governments also have begun testing post-quantum solutions. In 2022, the NATO Cyber Security Centre, responsible for the everyday protection of the alliance networks, successfully tested safe transmission flows using a virtual private network (VPN) supplied by the British firm Post-Quantum.

A VPN can utilize different algorithms provided by the manufacturer to ensure secure communications by guaranteeing that only the appropriate recipient of the data can read it.

Another method allies have experimented with is quantum key distribution, which consists of exchanging encryption keys, only known between the shared parties, that can be used to encrypt or decrypt further communications.

According to a NATO report on the subject, one of the distinct properties of this method is that it allows “only for the intended recipient to decode the message transmitted, making any eavesdropping impossible.”

In 2022, through this approach, a NATO Science for Peace & Security (SPS) project aimed to connect Malta and Italy for the first time with a prototype secure quantum communications undersea link featuring submarine, fiberoptic cables.

While quantum computing technology remains in its infancy, the importance for military organizations and the defense industry to get started now is to discover flaws in algorithms before they spread, thereby preventing widespread vulnerabilities in the future.

2.Are harvest now, decrypt later cyberattacks actually happening?

by Greg Noone
https://techmonitor.ai/hardware/quantum/harvest-now-decrypt-later-cyberattack-quantum-computer

The rationale behind post-quantum encryption is pretty simple. In about a decade's time – or sooner, if you're more optimistic – scientists will manage to build a quantum computer capable of harnessing hundreds of logical qubits. From there, it will be possible to build more powerful machines capable of cracking open any messages protected by current RSA encryption standards. At that moment, any country or company with a sufficiently powerful quantum computer could run riot across the internet and purloin national security secrets and sensitive corporate data at their leisure.

The more pressing concern is that this purloining may have already started. In so-called "harvest now, decrypt later" (HNDL) attacks, experts have theorised that rogue nation-states and cybercriminals could hoover up masses of encrypted data with the express intention of waiting until the moment when it can be decoded with great ceremony by a quantum computer. Some have implied that this is happening already. Earlier this month, for example, Deloitte's quantum readiness leader Colin Soutar was quoted in *Information Week* as saying that "[a]dversaries are targeting organizations via Harvest Now-Decrypt Later attacks."

It's a prospect that Western governments and companies are taking seriously. Since 2015, the US National Institute for Standards and Technology (NIST) has been working assiduously with cryptographers around the world on a set of post-quantum encryption standards capable of resisting the blunt force of tomorrow's quantum machines, standards that have been adopted by firms including Signal, Google, Thales and IBM, among others. In December, meanwhile, President Biden signed the Quantum Computing Cybersecurity Preparedness Act into law, which forced all federal agencies to develop plans to transition their systems to post-quantum encryption standards capable of surviving the arrival of 'Q-Day.' The UK government has issued its own gloomy advisories. Although a cryptographically relevant quantum computer (CRQC) does not yet exist, the National Cyber Security Centre wrote back in 2020, "the possibility of one is a relevant threat now to organisations that need to provide long-term cryptographic protection of data."

But *how* relevant? More specifically, are attackers actually now, right this minute, scooping up vast amounts of encrypted data to sit on until Q-Day?

So is harvest now, decrypt later a reality?

While many cybersecurity analysts and cryptographers are happy to attest to the threat of harvest now, decrypt later attacks, few are willing to openly claim that they're actually happening. For his part, Soutar wasn't willing to join the latter camp when *Tech Monitor* asked him to clarify his earlier comments to *Information Week*. "At Deloitte, we encourage clients to move away from guesswork about when a CRQC becomes available or from attempting to gauge the possibility of HNDL attacks," Soutar said, via email. "Instead, we recommend that organizations focus their efforts on understanding what their exposure might be and planning a migration to quantum-readiness and crypto-agility in an orderly manner."

In a similar vein, security vendor BlueVoyant's chairman Robert Hannigan warned the Slaughter and May podcast in 2021 that HNDL attacks were a "current problem," insofar that many companies are holding onto sensitive data – medical records, perhaps, or the specs for critical national infrastructure – that hostile actors would absolutely want to acquire and sit on in the hope that one day they can use a machine to read it properly. The ex-GCHQ director wasn't willing to go much further when *Tech Monitor* followed up with him last week.

"Data that is stolen is not going to be labelled 'for decryption later when quantum computers arrive'," said Hannigan, given that most of it is usually swiped in the name of short-term financial gain. "But it would be prudent to assume that hostile actors may be scooping up large amounts of encrypted data and may be storing it away for future decryption. That is at least a sensible working assumption."

Andersen Cheng is less circumspect. "You're speaking to the person who coined the phrase 'harvest now, decrypt later,'" says the founder of Post-Quantum, a cybersecurity start-up focused on quantum-safe encryption. "I started saying it back in 2015, and most people thought I was a lunatic."   No longer, says Cheng, who claims in our interview and elsewhere that the heads of multiple Western intelligence agencies have warned that HNDL attacks are happening "right in front of our eyes," so much so that the acronym has evolved into an initialism among US intelligence analysts ("They call it the 'handle.'")

How to pull off a HNDL attack

Diverting internet traffic through a border gateway protocol (BGP) hijack would be one way to do it, Cheng says. This type of attack, he explains, is the equivalent of tricking someone into driving to, say, Basingstoke along a series of B-roads where their car can be covertly photographed. They may get to their destination, and the photos may not even prove useful today, but someday, somehow, they will be — and the driver won't be any the wiser.

BGP rerouting failures are not uncommon, with traffic being diverted along zany routes thanks to various accidental ISP outages. Several cases, however, seemingly fit the profile of an HNDL attack. In 2016, for example, internet traffic heading to South Korea from Canada was mysteriously and repeatedly ending up in China. Four years later, data from over 200 networks belonging to the likes of Google, Facebook and Amazon was siphoned through Russia (a summary of these incidents can be found in this fantastic piece on post-quantum encryption by Rob Hastings.)

Are these the HNDL attacks we were warned about? Yuval Shavitt has co-written several papers over the years about these mysterious diversions, which the Tel Aviv University professor refers to as "deflection attacks." "Some of them are quite large-scale, which makes you wonder what is done with these large volumes of data," Shavitt tells *Tech Monitor*. Even so, he adds, "the purpose of any special deflection is beyond our ability to investigate."

Cheng himself concedes that he cannot definitively label any such incident as a HNDL attack, or recall any specific statement from Western intelligence agencies doing the same thing. "In fact, they would never do that," he says. "They will never pinpoint a specific incident, because then they would be giving away how they had detected it."

Are the security risks of quantum computers overhyped?

Harvest now, decrypt later attacks are certainly plausible, explains Ross Anderson, a professor of security engineering at Cambridge University. Just look at the Venona project, says Anderson, when the NSA spent decades decrypting thousands of Soviet messages it captured during the height of the Second World War. As far as modern-day surveillance is concerned, however, the cryptography expert is convinced that Western, Russian and Chinese agencies are much more interested in exploiting existing vulnerabilities in telecoms networks than they are acquiring masses of internet traffic and waiting until a quantum computer comes along to decrypt it.

“In addition to that, as 5G beds in, there will no doubt be various bugs and protocol misconfiguration and feature interactions and so on,” says Anderson. “The guys at KAIST keep on finding these, but it’s a hard job to do, because of the sheer complexity of the 5G specifications… it’s just too complicated for one person to understand it all.”

Perhaps unsurprisingly, Anderson is very much the quantum sceptic. “When it comes to civilian uses of cryptography, I think that the risks from quantum computers have been vastly overhyped,” he says. Skip Sanzeri takes the opposite view. The founder of QuSecure, Sanzeri earnestly believes that global cryptography needs the kind of makeover that only NIST-approved post-quantum algorithms can provide. But like Anderson, he doesn’t necessarily believe that we have to wait until the arrival of a CRQC before intelligence agencies based in Washington or Beijing can crack stolen encrypted data.

“A group called Memcomputing down in San Diego was tasked by the [US] Air Force under an SBIR to see if they could hack RSA 2048 with an ASIC chip,” says Sanzeri. On paper, at least, they claimed to have proved such decryption was possible. “This is no longer a quantum problem. Public key encryption? It’s done.”

Anderson seems less enthused. “People have been using ASICs [for decryption] for a generation,” he writes, referring to the use of the EFF DES Cracker chip (incongruously nicknamed “Deep Crack”) to brute-force a 56-bit key standard back in 1998.

It is, nevertheless, a timely reminder that some encryption standards are more vulnerable than others — though whether or not they are now prey to HNDL attacks remains, for now, impossible to confirm.

3.Quantum computer startup first to break 1000-qubit milestone

by Michael Irving
https://newatlas.com/computers/quantum-computer-startup-1-000-qubits/

A startup called Atom Computing has announced the first quantum computer to pass the 1000-qubit milestone. The prototype, due to become available for use in 2024, leapfrogs IBM’s announcement of its new quantum computer platform expected in the next few weeks.

Where traditional computers store and process information in binary states – either ones or zeroes – quantum computers allow data to exist in a superposition of both states at once. These quantum bits (qubits) give them a massive leg-up in computing power, allowing them to tackle traditional problems much faster and even take on tasks that would otherwise be impossible.

Now, Atom Computing has announced the most advanced quantum computing platform to date, boasting an impressive 1,180 qubits. That’s a huge leap over the previous most powerful quantum computer – IBM’s Osprey, with 433 qubits.

In Atom’s system, these qubits are ytterbium atoms, with lasers holding them in an array and manipulating their states to store and process data. The company says that ytterbium is the ideal candidate for the job, since it only has two quantum levels in its lowest energy state, meaning it’s easier to manipulate and measure than other atoms.

Atom claims that its quantum computer excels in other measures too. Earlier this year the company demonstrated mid-circuit measurement – where the quantum state of desired qubits can be probed without disturbing neighboring qubits. The computer also apparently boasts coherence times – a measure of how long qubits can store information – of 40 seconds. By comparison, the Osprey tops out at around 80 microseconds.

While it may sound like Atom has left other companies in the dust, the race is closer than you might think. IBM's multi-year roadmap suggests the company will announce its own quantum computer surpassing the 1,000-qubit mark in the next few weeks with the Condor, running 1,121 qubits.

Atom Computing says that it will begin allowing enterprise, academic and government users access to its quantum computer systems in 2024.

4.How the US is Preparing For a Post-Quantum World

by Nick Polk
https://news.slashdot.org/story/23/10/28/1655259/how-the-us-is-preparing-for-a-post-quantum-world

The U.S. is in the early stages of a major shift focused on bolstering government network defenses, pushing federal agencies to adopt a new encryption standard known as post-quantum cryptography that aims to prevent systems from being vulnerable to advanced decryption techniques enabled by quantum computers in the near future.

We've been using asymmetric encryption for a very long time now, and it's been ubiquitous since about 2014, when the U.S. government and some of the large tech companies decided that they're going to make it a default on most web browsers... Interestingly enough, regarding the post-quantum cryptographic standards being developed, the only thing that's quantum about them is that it has "quantum" in the name. It's really just a different type of math that's much more difficult for a quantum computer to be able to reverse-engineer. The National Institute of Standards and Technology is looking at different mathematical models to cover all their bases. The interesting thing is that these post-quantum standards are actually being used to protect classical computers that we have now, like laptops…

Given the breadth of the U.S. government and the amount of computing power we use, we really see ourselves and our role as a steward of the tech ecosystem. One of the things that came out of [this week's Inside Quantum Technology conference in New York City] was that we are very quickly moving along with the private sector to migrate to post-quantum cryptography. I think you're gonna see very shortly a lot of very sensitive private sector industries start to migrate or start to advertise that they're going to migrate. Banks are a perfect example. That means meeting with vendors regularly, and testing their algorithms to ensure that we can accurately and effectively implement them on federal systems…

The administration and national security memorandum set 2035 as our deadline as a government to migrate our [national security] systems to post-quantum cryptography. That's supposed to time with the development of operational quantum computers. We need to ensure that we start now, so that we don't end up not meeting the deadline before computers are operational... This is a prioritized migration for the U.S. government. We're going to start with our most critical systems — that includes what we call high-value assets, and high-impact systems. So for example, we're gonna prioritize systems that have personal health information.

That's our biggest emphasis — both when we talk to private industry and when we encourage agencies when they talk to their contractors and vendors — to really think about where your most sensitive data is and then prioritize those systems for migration.

5.ExpressVPN launches post-quantum protection

by Chiara Castro
https://www.techradar.com/computing/cyber-security/expressvpn-launches-post-quantum-protection

After unveiling a feature-packed update only a week ago, TechRadar's best VPN service decided to scale up its encryption as quantum computing's threats loom.

ExpressVPN's speedy and secure VPN protocol now includes post-quantum protections by default across its Android, iOS, Linux, Mac, and Windows apps. Users need to just update their applications to the latest version to enjoy the additional layer of encryption.

An early pioneer in the VPN industry, the provider seeks to play an active role in the transition to a quantum-safe world. "We are proud to be innovators who are helping to lead the charge for a quantum-safe future in the VPN industry," Pete Membrey, Chief Engineering Officer at Express told me.

ExpressVPN's post-quantum protections

As quantum computers get widely accessible, end-to-end encryption is at risk of becoming obsolete. That's because quantum computing machines can process exponentially more complex processes in just a fraction of the time compared to classical computers, including breaking into today's encrypted layers.

This may be a decade away still. Yet, "harvest now, decrypt later" attacks are already threatening people's data. "We believe it is important to stay ahead of the clock and put in protections before quantum computing becomes an immediate threat," said Membrey.

He and his team of engineers knew this already back in 2020 when they were designing the ExpressVPN Lightway protocol completely in-house. For those unfamiliar with this technology, a VPN protocol refers to the method of encryption used to protect your data.

Membrey's team decided to keep standard transport layer security (TLS) and datagram TLS (DTLS) implementations, knowing that the DTLS 1.3 update would bring about the needed extension to support more advanced things like post-quantum keys. They then turn to the open-source WolfSSL cryptography library for its higher speeds which would come in handy when adding more complex features.

"When WolfSSL added support for DTLS 1.3, and also integration with the Open Quantum Safe library, it was relatively straightforward for us to upgrade," Membrey told me, adding that the real work was instead ensuring all the features were secure and reliable.

"That ended up being hundreds of hours of testing and refinement, and a close collaboration with WolfSSL to perfect their implementation for our heavy use case. Once we were confident in our testing, rolling it out was as simple as deciding to enable the feature."

Express' WireGuard-inspired protocol is now utilizing algorithms integrated from the Open Quantum Safe team's liboqs (P256_KYBER_LEVEL1 for UDP and P521_KYBER_LEVEL5 for TCP). Kyber was actually chosen by the National Institute of Standards and Technology (NIST) as the candidate for general post-quantum encryption. Even better, being the protocol open-sourced, everyone can check the new code.

Post-quantum technology is still relatively new, less battle-tested, and unpredictable compared to classical cryptographic algorithms. That's why the provider decided to blend both new and old encryption keys for now, letting them work together in a hybrid mode harmony.

Membrey said: "A hybrid approach means that users are safe from attacks by classical computers without relying on post-quantum algorithms, and they also have the best chance we know of today of being safe from attacks by quantum computers.”

He confirmed the intention of continuing to lean to the open-source community—ExpressVPN's Lightway protocol, WolfSSL's cryptographic libraries, and the liboqs project are all open-sourced, in fact—to keep evolving Express' post-quantum solutions as the computing space progresses.

The post-quantum race

ExpressVPN might be one of the first VPNs to have implemented post-quantum cryptography, but it's certainly not the only security software provider walking in the same direction.

Secure email services have already started raising their encryption wall, too. Hannover-based Tutanota announced its project to bring post-quantum cryptography to the cloud back in July, securing a grant and partnership with the University of Wuppertal.

This week, Proton (the firm behind homonymous VPN, email, and drive services) announced that it's working on quantum-safe encryption algorithms in OpenPGP. The open standard of encryption, the company said it's available for anyone to use via the free and open-source libraries which it maintains, such as OpenPGP.js and Gopenpgp.

About a month ago the popular messaging app, Signal, added quantum-level encryption to its security infrastructure with its latest update. PureVPN beat many to the punch by rolling quantum-resistant keys back in April 2022.

The race for post-quantum encryption has officially begun—and the time has never been so crucial. Every cryptographer is probably fighting against the clock to solve this quest by now. Yet, Membrey believes Express could have an advantage that many VPNs may not have.

"Lightway was designed specifically to allow us to make such modifications in a simple and standard way," he says. "Other VPN protocols would need extensive changes to support post-quantum. There are options available, but they are effectively extensions to, or workarounds for the existing protocols. None offer the seamless support that Lightway can offer."

6.Time to get serious about the dangers of quantum computing

by John Thornhill

https://www.ft.com/content/9ac38cf4-874e-4842-8be9-8fac2a3e898d

The old joke that quantum computing is a technology of the future — and will forever remain so — is not so funny any more.

The engineering challenges of building a quantum computer robust enough to deliver on its extraordinary theoretical promise remain colossal. But early prototypes are evolving fast and the future might arrive quicker than predicted. Every data-rich body should start thinking about how to migrate to a quantum world now the US National Institute of Standards and Technology is due to release its post-quantum encryption standards next year.

Quantum computers, which exploit the spooky behaviour of subatomic physics, operate in a different way from conventional computers, enlarging the set of possible solutions to many problems. Some companies are already exploring the possibilities of hybrid approaches, combining the existing capabilities of rudimentary quantum computers and their classical cousins to optimise port logistics, airline schedules, grocery deliveries and television advertising programming, for example.

“Quantum is real today,” says Alan Baratz, chief executive of D-Wave, a Canadian quantum company.

But the serious threats of quantum computing may emerge quicker than its possibilities. Security experts warn of the dangers of Q-day, when a quantum computer might crack the RSA cryptosystem, widely used by tech companies, banks and governments on their data.

Earlier this month, the heads of the “Five Eyes” spy agencies (the US, the UK, Canada, Australia and New Zealand) warned of the risks of China’s activities in quantum computing, AI and synthetic biology. “If you’re anywhere close to the cutting edge of tech, you might not be interested in geopolitics, but geopolitics is interested in you,” said Ken McCallum, director-general of Britain’s MI5.

Ever since 1994, when the mathematician Peter Shor wrote an algorithm that could run on a not-yet-invented quantum computer to crack RSA, security experts have worried about the world’s digital secrets. It may be another decade (or more) before we have a quantum computer stable enough to run Shor’s algorithm but we can never be certain when that day might arrive.

This is one of those rare technological fields, however, where the solution anticipates the problem. Since 2016, America’s National Institute has been soliciting and evaluating quantum-proof encryption. It will release four approved standards next year, which will then be adopted by other agencies around the world.

According to Elham Kashefi, chief scientist at the UK’s National Quantum Computing Centre, it would be “very worrisome” if any organisation that holds sensitive data was not already alert to the threat of Q-day. “You should be very worried,” she told the Sifted Summit earlier this month.

One concern was that adversaries could harness data today and decrypt it later when quantum computers had developed, Kashefi said. That might not matter if the old, compromised data was a supermarket’s daily sales records. But it would be a different story if the data contained health records or sensitive personal information.

Switching from one encryption regime to another across many thousands of organisations will take years to implement. That is why cyber experts are urging companies to start thinking now about how to adopt a NIST-approved encryption standard.

Migrating to a quantum-proof world will be a bonanza for some cyber security companies. That is the hope of PQ Shield, an Oxford-based start-up that recently convened an expert conference to examine whether NIST's "beautiful" mathematical drafts could work in the "nasty" hardware world. The good news, according to Ali El Kaafarani, PQ Shield's founder, is that they can.

"Is there ever a perfect security solution? No. It never exists," he tells me. "But my personal view is that these schemes are very secure and strong and very difficult to break on either a classical or a quantum computer."

When I spoke to Shor earlier this year, he predicted that the quantum computer needed to run his algorithm might still be decades away. But in the meantime, he had composed a limerick to explain the quantum conundrum:

"If the computers you build are quantum,

Spies of all factions will want 'em.

Our codes will all fail.

They'll read all our email.

Till we've crypto that's quantum and daunt 'em."

7.Quantum Synergy: Enabling Groundbreaking Research in National Labs with Quantum Computers

by Pedro Lopes
https://quantumcomputingreport.com/quantum-synergy-enabling-groundbreaking-research-in-national-labs-with-quantum-computers/

National laboratories have long been at the forefront of scientific and technological innovation, playing a crucial role in accelerating progress. Their infrastructure, established during the Second World War and continuously evolving since, has enabled significant discoveries in areas such as nuclear energy, weather forecasting (including climate change), and materials development for battery and carbon capture technologies, addressing pressing challenges faced by humanity.

From their inception, national labs have recognised the importance of high-performance computing. They were early adopters of supercomputing technologies that emerged in the 1960s and 1970s, positioning them as leaders in complex modelling, simulation, and data analysis. These capabilities have been instrumental in facilitating major discoveries, as well as in the training of sophisticated contemporary artificial intelligence models.

This visionary mindset also drove national labs to develop a keen interest in the recent emergence of quantum computers. Although still in relative infancy, quantum computing promises exponential advancements in computational power, leveraging the principles of quantum mechanics. Whether for simulating novel materials, improving machine learning capabilities, or predicting extreme weather events, quantum computing capabilities can contribute to existing research directions and open up new ones.

Access to diverse quantum computing platforms is paramount from a national lab perspective. Quantum computers today come in various technologies—superconducting qubits, trapped ions, photonics, and neutral atoms—each with distinct advantages and potential use cases. Today, no single platform is best suited for all problems. Providing access to a range of computers and modalities ensures that researchers have the best tools to meet their diverse research needs and fosters resilience in this rapidly evolving field.

A crucial question is how to best provide such access: whether on-premises or via the cloud. On-premises quantum computers offer advantages such as full control over scheduling and availability, reduced reliance on external connectivity, data protection for sensitive applications, tighter integration with existing classical computing resources, and opportunities for custom modifications. They also facilitate in-house development of the expertise required to operate and maintain these cutting-edge machines. Remote access, on the other hand, offers flexibility, reduces initial capital outlays, outsources the management and maintenance activities to cloud providers, and protects against rapid obsolescence of on-premises systems. The optimal choice depends on the specific circumstances of each Lab.

Beyond hardware access, national labs can benefit from direct access to the scientists who develop and maintain quantum computers. Such scientists, often employed by quantum computing vendors, provide invaluable expertise and assistance in managing quantum infrastructure. These experts possess in-depth knowledge of their machines and stay at the forefront of quantum computing research. They can help decide which problems are a good fit for today's quantum computers and assist in the optimal mapping of the problem to the capabilities of the hardware. In the case of neutral-atom computers, some of which can uniquely operate in both analog computing mode and digital gate-based mode, this expertise becomes even more critical due to the added complexity and flexibility.

At QuEra, we actively foster relationships with U.S. National Labs, exemplifying the value of close partnerships in designing optimal quantum computing services tailored to their needs. Through a collaborative effort, we have provided one such lab with access to our cutting-edge neutral atom quantum computer. The primary objective of this particular collaboration was to empower the lab's quantum team to become proficient in our quantum computing technology, enabling them to subsequently allocate computing resources and technical support to their own user community. Our partnership revolves around a joint project, offering the lab's team hands-on experience and direct technical guidance from our experts in a real-life setting, simulating their future interactions with the scientists they will serve. The project was also designed to strategically use quantum dynamics simulations – the key strength of QuEra's Aquila – to address a problem that simultaneously impacts the chemistry, materials, and high-energy physics communities, arguably the main audiences that the US national labs cater to. Through further community-building activities, including training and brainstorming sessions with the lab's larger user base, we help set the lab's quantum program for success. Through this design, our collaboration with the lab's developers has rapidly expanded, with interest from scientists growing five-fold in just a few months, underscoring the relevance and appeal of our resources.

We have addressed specific research inquiries through ongoing interaction and collaboration, tailored our system to meet the lab's requirements, and collectively overcame challenges. The feedback and insights gained from this collaboration have been invaluable in refining our technology and shaping our future development plans, and of course have also been very valuable to the lab itself. This symbiotic relationship enhances the lab's research capabilities and advances our understanding and progress in neutral-atom quantum computing. Such real-world experiences highlight the immense potential of collaborative endeavors.

We made our cloud resources available to a different national lab in a separate project. That lab now has access to superconducting, annealing, trapped ions, and now neutral-atom computers. It allows them to benchmark different modalities and make recommendations to their users on what the most appropriate resource is for any given problem. QuEra also benefited from this interaction, providing us a better understanding of the scheduling, reporting, and billing requirements of a sophisticated user.

A collaborative approach, where vendors closely work with national labs to understand their needs, provide appropriate hardware, and offer ongoing expert support, brings significant benefits. It creates a virtuous cycle where lab feedback informs future hardware and software developments, and lab discoveries push the boundaries of what is possible with quantum computers. Such cooperation not only accelerates progress within each national lab but also contributes to the collective quantum computing capabilities of the broader scientific community. It ensures that these powerful tools are not limited to a select few but are accessible to a diverse array of researchers working on society's most pressing scientific challenges.

Furthermore, it's important to note that the connection between quantum computing and traditional supercomputing resources is being beyond our borders. Several organizations in the European Union chose to strategically pursue high-performance computing developments since the early 2010s. White papers identifying trends and needs for heterogeneous computing environments, including quantum nodes alongside CPUs and GPUs, have been published. This planning has manifested in recent moves by leading European high-performance computing centers, both public and private, to acquire quantum computing nodes. Notably, the Jülich Supercomputing Center in Germany has made significant efforts in this regard, and the EuroHPC program has designated six different countries to purchase six different quantum computers for shared exploration.

In conclusion, national laboratories play a vital role in driving scientific and technological progress, and quantum computers hold immense potential to accelerate this progress. By providing these institutions with access to diverse quantum computing platforms and expert guidance, hardware developers not only contribute to advancing the labs' missions but also enhance their own ability to offer quality services that address society's challenges through quantum computing. The pursuit of such relationships is a global trend, and national labs that wish to continue to be beacons of innovation and research leadership must continue to invest in quantum computing integration.

8.Quantum computers in 2023: how they work, what they do, and where they're heading

by Christopher Ferrie
https://theconversation.com/quantum-computers-in-2023-how-they-work-what-they-do-and-where-theyre-heading-215804

In June, an IBM computing executive claimed quantum computers were entering the "utility" phase, in which high-tech experimental devices become useful. In September, Australia's Chief Scientist Cathy Foley went so far as to declare "the dawn of the quantum era".

This week, Australian physicist Michelle Simmons won the nation's top science award for her work on developing silicon-based quantum computers.

Obviously, quantum computers are having a moment. But – to step back a little – what exactly *are* they?

What is a quantum computer?

One way to think about computers is in terms of the kinds of numbers they work with.

The digital computers we use every day rely on whole numbers (or *integers*), representing information as strings of zeroes and ones which they rearrange according to complicated rules. There are also analogue computers, which represent information as continuously varying numbers (or *real numbers*), manipulated via electrical circuits or spinning rotors or moving fluids.

In the 16th century, the Italian mathematician Girolamo Cardano invented another kind of number called *complex numbers* to solve seemingly impossible tasks such as finding the square root of a negative number. In the 20th century, with the advent of quantum physics, it turned out complex numbers also naturally describe the fine details of light and matter.

In the 1990s, physics and computer science collided when it was discovered that some problems could be solved much faster with algorithms that work directly with complex numbers as encoded in quantum physics.

The next logical step was to build devices that work with light and matter to do those calculations for us automatically. This was the birth of quantum computing.

Why does quantum computing matter?

We usually think of the things our computers do in terms that mean something to us — balance my spreadsheet, transmit my live video, find my ride to the airport. However, all of these are ultimately computational problems, phrased in mathematical language.

As quantum computing is still a nascent field, most of the problems we know quantum computers will solve are phrased in abstract mathematics. Some of these will have “real world” applications we can’t yet foresee, but others will find a more immediate impact.

One early application will be cryptography. Quantum computers will be able to crack today’s internet encryption algorithms, so we will need quantum-resistant cryptographic technology. Provably secure cryptography and a fully quantum internet would use quantum computing technology.

In materials science, quantum computers will be able to simulate molecular structures at the atomic scale, making it faster and easier to discover new and interesting materials. This may have significant applications in batteries, pharmaceuticals, fertilisers and other chemistry-based domains.

Quantum computers will also speed up many difficult optimisation problems, where we want to find the “best” way to do something. This will allow us to tackle larger-scale problems in areas such as logistics, finance, and weather forecasting.

Machine learning is another area where quantum computers may accelerate progress. This could happen indirectly, by speeding up subroutines in digital computers, or directly if quantum computers can be reimagined as learning machines.

What is the current landscape?

In 2023, quantum computing is moving out of the basement laboratories of university physics departments and into industrial research and development facilities. The move is backed by the chequebooks of multinational corporations and venture capitalists.

Contemporary quantum computing prototypes – built by IBM, Google, IonQ, Rigetti and others – are still some way from perfection.

Today's machines are of modest size and susceptible to errors, in what has been called the "noisy intermediate-scale quantum" phase of development. The delicate nature of tiny quantum systems means they are prone to many sources of error, and correcting these errors is a major technical hurdle.

The holy grail is a large-scale quantum computer which can correct its own errors. A whole ecosystem of research factions and commercial enterprises are pursuing this goal via diverse technological approaches.

Superconductors, ions, silicon, photons

The current leading approach uses loops of electric current inside superconducting circuits to store and manipulate information. This is the technology adopted by Google, IBM, Rigetti and others.

Another method, the "trapped ion" technology, works with groups of electrically charged atomic particles, using the inherent stability of the particles to reduce errors. This approach has been spearheaded by IonQ and Honeywell.

A third route of exploration is to confine electrons within tiny particles of semiconductor material, which could then be melded into the well-established silicon technology of classical computing. Silicon Quantum Computing is pursuing this angle.

Yet another direction is to use individual particles of light (photons), which can be manipulated with high fidelity. A company called PsiQuantum is designing intricate "guided light" circuits to perform quantum computations.

There is no clear winner yet from among these technologies, and it may well be a hybrid approach that ultimately prevails.

Where will the quantum future take us?

Attempting to forecast the future of quantum computing today is akin to predicting flying cars and ending up with cameras in our phones instead. Nevertheless, there are a few milestones that many researchers would agree are likely to be reached in the next decade.

Better error correction is a big one. We expect to see a transition from the era of noisy devices to small devices that can sustain computation through active error correction.

Another is the advent of post-quantum cryptography. This means the establishment and adoption of cryptographic standards that can't easily be broken by quantum computers.

Commercial spin-offs of technology such as quantum sensing are also on the horizon.

The demonstration of a genuine "quantum advantage" will also be a likely development. This means a compelling application where a quantum device is unarguably superior to the digital alternative.

And a stretch goal for the coming decade is the creation of a large-scale quantum computer free of errors (with active error correction).

When this has been achieved, we can be confident the 21st century will be the "quantum era".

9.AWS claims quantum networking break-

through

by Ryan Morrison
https://techmonitor.ai/hardware/quantum/aws-claims-quantum-networking-breakthrough

AWS says it has made a breakthrough in quantum networking that could also boost the speed and efficiency of classical telecom networks. Working with Harvard University, researchers at Amazon's cloud platform created a new packaging method for optical fibres that solves a long-standing problem with data degradation at a distance.

Quantum communication is a rapidly advancing field as the world moves from classical to post-quantum cryptography standards and from metal to light-based networking cables. The problem is that fibre optic cable systems struggle with data degradation over long distances, particularly when working with quantum data or in extreme temperature environments. These include issues connecting a fibre and a device on a larger scale, developing light modulators for high-speed classical communication, or co-packaged optics for data centres.

There have been experiments with new types of cable and entanglement systems recently, including one between the UK and Ireland to try and solve this problem. In some cases it involves the addition of new equipment to encode the data, other solutions involve network packaging.

Why packaging is key to quantum communication

In optical networking, packaging is a key component and an active area of research. It is the process of housing or enclosing optical components such as lasers, detectors, or fibres in a manner that protects them, ensures their correct alignment, and facilitates their interaction or connection with other components. It is felt improved packaging holds the key to solving the distance problem for quantum networking.

Light in optical fibres is confined to a region with a diameter of a fraction of the size of a single human hair. This creates a fragile environment with extremely precise alignment of components, which can easily be disrupted. This becomes especially challenging for low-temperature operations used by many quantum devices. For AWS, improving the packaging is an important step towards the goal of creating a system that works in all environments, including where cables may be laid across a road.

Central to this is packing the fibre optic cable with quantum repeaters that can re-encode data, correct photon loss in real-time and do so without disrupting the quantum nature of the information being carried down the fibre optic cable.

In the new AWS method, a tapered end of the optical fibre is put in physical contact with a tapered end of the optical device, such as the quantum repeater, allowing light to gradually pass through the interface. Forces between tapered ends give the interface immunity against small displacements of the components, such as if it is buried under a road and the noise of the traffic causes minor disruptions in the placement of the cable.

As well as working at cryogenic temperatures, AWS scientists say that this can also be packaged with the types of modulators used in high-speed telecommunication networks. As quantum computers and quantum networking become more common, it could also allow cheaper and more efficient interfaces between quantum and classical hardware.

10.Scaling up prime factorization with self-organizing gates

by Kevin Townsend

https://www.securityweek.com/beyond-quantum-memcomputing-asics-could-shatter-2048-bit-rsa-encryption/

MemComputing is a company and computing philosophy born out of theory. The theory is that if processing and data can be combined in memory, the so-called 'von Neumann bottleneck' can be broken. This bottleneck is latency introduced by having storage and processing separate, and the consequent necessity of communicating between the two.

As the computational complexity increases, the processing time required by classical computers also increases – but exponentially. The result of the bottleneck is that a category of complex mathematical problems cannot be solved by classical (basic von Neumann architecture) in any meaningful time frame.

"Among intractable combinatorial problems, large-scale prime factorization is a well-known challenge," MemComputing researchers wrote in a paper titled *Scaling up prime factorization with self-organizing gates: A memcomputing approach* (PDF). It is the intractability of this problem that has kept RSA-based encryption theoretically secure for so long. It's not that it is mathematically impossible, merely that it would take too long to be realistic using classical computers.

Where theory cannot be demonstrated by fact, the problem and solution are emulated in software. For cracking RSA, "Presently, sieve methods represent the state-of-the-art algorithms showing promise, with the general number field sieve method being the most effective. Nevertheless, even these methods struggle to factor a 2048-bit RSA key within a sensible timeframe, and past instances have taken almost 2700-CPU-years to factor an 829-bit number using computer clusters."

The von Neumann bottleneck means that time-to-solution increases exponentially. "It is estimated that with current technology using the best-known algorithm (general number field sieve, GNFS), factoring a 2048-bit RSA key would take longer than the age of the universe," the researchers added.

Quantum computers will be able to solve this problem within a meaningful timeframe. Hence the NIST-driven drive for more complex post-quantum algorithms able to continue protecting encryption. Estimates of the arrival of quantum computers vary greatly, but 'decades' is usually quoted.

Enter MemComputing's combined memory/processing. Simulation shows that the complexity/time ratio for solving difficult problems increases only polynomially rather than exponentially. In other words, difficult problems can be solved very much faster — and the time taken to do so can be massively reduced.

MemComputing effectively wanted to know how long it would take its patented in-memory processing to crack RSA, and whether it could be done in a shorter timeframe than waiting for the arrival of quantum computers. The basic study resulted from a Small Business Innovation Research (SBIR) contract with the US Air Force.

The approach taken was to use software emulation focusing on test problems from 30 to 150 bits. "Results showed that the circuit generated the appropriate congruences for benchmark problems up to 300 bits, and the time needed to factorize followed a 2nd-degree polynomial in the number of bits," MemComputing announced. In other words, the increasing complexity of factoring large numbers with in-memory computing increases the necessary time far more slowly than the exponential increase afforded by classical computers.

“The next step is to extend the effective range beyond 300 bits, which requires customizing the SOG design to even larger factorization problems, with the end goal of realizing the capability in an Application Specific Integrated Circuit (ASIC),” continued the company.

An ASIC is a custom chip. They are already widely used for different applications. They take longer and are more costly to produce than general purpose classical computer chips, but neither are in the same league as developing and waiting for a quantum computer.

Specifically, the researchers said, “The timing for the ASIC realization of the MEMCPU Platform is also reported. The ASIC timing can be easily estimated since the MEMCPU Platform, being a circuit emulator, returns the full dynamics of the circuit, including the simulated runtime. It is worth noting that, at this point in our R&D, the forecast for the ASIC shows the possibility of solving a 2048-bit factorization problem in tens of minutes.”

This conclusion is, of course, theory rather than demonstrable fact. The theory, however, is based on a body of fact, and theoretical research underlies much of today’s demonstrable science. If it all proves practical, the feared ‘cryptopocalypse’ (the death of current encryption) might be sooner than expected – caused by in-memory computing ASICs rather than quantum computers.

11.The U.S. Approach to Quantum Policy

by Global Quantum Intelligence
https://quantumcomputingreport.com/recommended-reading-the-u-s-approach-to-quantum-policy/

The $1.2 billion U.S. National Quantum Initiative (NQI) was enacted in December 2018 for a ten year period with budget authorizations for science activities specified only for the first five fiscal years which ended on September 30, 2023. Although the U.S. Congress has a lot of issues to work through first, like the full government’s budget for FY2024, we do expect that will be get around to renewing the NQI in one form or another later this year. Support for quantum technology is one issue that carries support from both sides of the political aisle.

The House Committee on Science, Space, and Technology held a hearing on this topic in June of this year and we had published some of our recommendations a few days after that hearing. In addition, the U.S. National Quantum Initiative Advisory Committee (NQAIC) issued a report with their findings which we summarized in an article here.

Now, the Center for Data Innovation has published a comprehensive report that provides ten recommendations for policy action by Congress. The report includes a background on some of the previous quantum research funding from the U.S. government, a description of key quantum research centers supported by the National Science Foundation (NSF) and the Department of Energy (DOE), a brief description of quantum research support by the UK, Canada, and the European Union, and recommendations for a renewed NQI. These NQI recommendations include a funding level of at least $525 million per year for the next five fiscal years, support for providing researcher access to quantum computing resources, education and workforce development programs, a supply chain study, and international cooperation.

Although the U.S. government was one of the earliest funding of quantum technology research, in recent years the U.S. has been lagging behind a few other countries. The report maintains that having a strong quantum technology ecosystem is strategically crucial for the United States in terms of both its economic and societal well-being and that the U.S. government should take proactive measures immediately to maintain its leadership position

The full report is titled *The U.S. Approach to Quantum Policy* and it can be accessed on the website of the Center for Data Innovation here.

12.China's Photonic Jiuzhang Series Sets (Yet Another) Speed Record

by Matt Swayne
https://thequantuminsider.com/2023/10/12/chinas-photonic-jiuzhang-series-sets-yet-another-speed-record/

The fast-moving realm of quantum computing just got faster as scientists in China unveil the latest results from the JiuZhang photonic quantum computer series, which reportedly solved a complex mathematical problem in a mere millionth of a second. According to a recent story in the South China Morning Post, the feat outpaces the world's fastest supercomputer by a staggering margin, performing the calculation over 20 billion years quicker than its supercomputer colleague.

The research team, spearheaded by the Pan Jianwei[1] from the University of Science and Technology of China in Anhui province, introduced the JiuZhang 3 prototype, which surpassed the record set by its earlier version with a calculation speed that's accelerated by a factor of one million. The researchers released their findings in a paper published in the Physical Review Letters on Tuesday.

Named after an ancient Chinese mathematical text, the JiuZhang series uses photons as the computational medium and leverages the fundamental quantum information unit: the qubit. The JiuZhang series has developed significantly over the last few years. With the inaugural JiuZhang machine in 2020 utilizing 76 photons, and its successor operating with 113, the latest iteration has 255 photons, the SCMP reports.

This advance in photon utilization was implemented to navigate a perplexing problem grounded in Gaussian boson sampling, a paradigm that simulates the intricate behaviors of light particles as they traverse through a complex labyrinth of crystals and mirrors. Originally conceptualized as essentially a purposeless physical game, recent scholarly investigations suggest that boson sampling could harbor potential applications in the intricate field of cryptography, according to the news site.

The latest news about JiuZhang 3 solidifies China's position as a global quantum leadership. The international photonic quantum space has several leaders, though, including Xanadu, a Toronto-based company. Xanadu, for instance, writes in 2022 that its Borealis photonic QC has 216 squeezed-state qubits — and it's available on the public cloud.

Even with global quantum computer developers breaking speed records, some critics have charged that many of these announcements are largely ceremonial. Boson sampling is a toy problem that might not serve as a great benchmark for future practical quantum computing use cases. First, boson sampling tasks are ideally suited for quantum computers to outperform classical computers. In fact, the task even more suited for photonic quantum computers. Second, besides the potential to use in cryptographic

[1] Pan Jianwei is often referred to as the father of China's quantum program.

methods, the critics say that boson sampling has little real world applications.

Other quantum computer researchers have recognized this and have become less worried about breaking speed records and more interested in pursuing practical quantum advantage at tasks that would have more immediate commercial applications, such as drug discovery and financial optimization problems.

13.Why a cryptographer can be your org's secret weapon

by Jeremy Bradley
https://www.siliconrepublic.com/enterprise/cryptographer-skills-digital-privacy-codes-data-zama

There is a paradox when it comes to cryptography. Most people have come to know cryptographers through representations of real-life events and fiction: you went to the movies to see Alan Turing defeating the Enigma machine, read about Sherlock Holmes cracking codes to solve cases and cheered for hackers using their skills for a good cause.

These portrayals present cryptography as a cool game of cat and mouse, solving enigmas and deciphering secret communications. Though this is all true and accurate, these depictions don't explore the full extent of what cryptography is nor how important it has become in our digital lives.

Cracking the right profile

Cryptographers are indeed experts in unveiling secret codes and solving enigmas, but more than anything they are professionals trained to identify and forecast potential threats and devise tailored preventive solutions.

They must have specific skills and characteristics, such as having a strong background in and knowledge of mathematical sciences as well as good implementing skills. Most of these skills would have been acquired through their studies, with a math or computer science degree being essential – a background in engineering might also help and a PhD would further support someone looking to become a cryptographer or cryptanalyst.

Less predictable skills, but still extremely valuable, can also contribute to shaping a well-rounded professional in the field. Good intuition and communication skills can be extremely helpful when working in a team to solve complex problems, and, obviously, a real passion for privacy and a commitment to delivering solutions in the field.

Cryptography, the 'science of security', has come a long way over the last two decades or so, from public-key systems, such as RSA and elliptic curve cryptography (ECC), focusing on data transmission, to multiparty computation (MPC) and fully homomorphic encryption (FHE), which enables data to be processed without having to decrypt it.

With new and improved forms of cryptographic techniques being developed constantly, cryptographers also need to be open-minded and flexible to adapt to different problems and solutions as demands arise.

Who needs a cryptographer?

When looking below the surface, it becomes clear that cryptographers are much more complex figures than you might think. What is still too frequently overlooked is the importance of their role in businesses and organisations across different industries, applying their particular expertise and abilities to add value to services and products.

Here are some of businesses that should employ cryptographers and what this role could bring to the table.

Financial services

Banks and providers dealing with online payments require strong protection to deliver secure transactions. Sensitive data are held (account numbers, personal information, access and PIN codes) to allow the movement of money between customers and the institution.

Cryptographers ensure that encryption measures are in place to keep transactions and information private and authentic when operating remotely. Cryptography is also at the very heart of blockchain and decentralised finance (DeFi).

Market research and statistics

Market analysis and forecasts usually focus on evaluations, profits and investments, but when the information gathered is sensitive data then there is a clear need for privacy and protection.

Organisations that collect personal identifiable information (PII) for statistical purposes (names, addresses, contacts and so on) can employ cryptographers to make sure that the statistical data are stored while guaranteeing that nobody can access or modify the original information.

Software companies

Cryptographers are problem-solvers thanks to their maths training, and, thanks to their computer training, they are developers: their mindset is to try and anticipate the potential attacks and then create the appropriate defensive measures.

Companies developing software for applications, systems or drivers need cryptographers to protect their intellectual property and know-how. Cryptographers also ensure that whatever data and information that is processed by the end product will be private and authenticated.

Gaming

With the rise in popularity of home and online gaming, big game developers have found themselves facing new and evolving threats to their creations.

Digital rights management (DRM) has become a priority, necessary to protect games from being copied or distributed through unauthorised channels.

When you provide a device to people, piracy becomes more likely. Your user is now also a potential attacker. However, if you involve cryptographers from the early stages of game development, you will ensure all the right protections are in place.

Cloud services

Protecting cloud communication and data storage requires a combination of different elements: tackling personal activities, monitoring server users, accessing browsers and apps, and protecting communication between users and providers.

With so much data in the cloud, you need to make sure this can't be seen or hijacked, stolen or misused.

Many of the measures already in place have been developed by cryptographers using a plethora of techniques, which include different forms of encryption, secure channels, digital signatures and two-factor authentication. This ensure that anything exchanged cannot be exploited and that users are indeed accountable for their actions.

Focus on privacy

Cryptographers are highly skilled and well-placed to educate people about the importance of privacy and work on developing the field.

The research and teaching field is not one to overlook: this is where the culture for privacy is cultivated, where the science of security keeps growing and evolving, and where new generations of cryptographers are trained to face the challenges that will be brought on by the continued advancements in technology.

The constant evolution of technologies and ways to collect, store and share information highlights why businesses and organisations should add cryptographers to their workforce. Their contribution goes beyond simple cybersecurity or IT infrastructure. In fighting threats and securing the latest privacy standards are met and challenges overcome, cryptographers can be your organisation's secret weapon.

14.Standards Body Considers Uncloaking Secret Encryption Algorithms

by Kim Zetter
https://www.zetter-zeroday.com/p/standards-body-considers-uncloaking

A European standards body that found itself in hot water this summer over flaws in encryption algorithms it created to secure radio communications of police, military and critical infrastructure, is now discussing whether to make its new algorithms public as a result of the backlash, I've learned.

The European Telecommunications Standards Institute (ETSI) has put the question to members and is seeking consensus this month on whether new proprietary algorithms it has created for the TETRA radio protocol should be made public so that independent researchers and government agencies that rely on the algorithms to protect their communications can examine them for security flaws. If members can't come to a consensus informally, the group is expected to put the matter to a vote on October 26.

ETSI spokeswoman Claire Boyer confirmed that the group is weighing whether to make the new algorithms public.

"The question as to whether TETRA algorithms will be made public is still open at this time," she wrote in an email. "Resolution is expected from ETSI TCCE technical committee in charge of TETRA by the end of the year."

Matthew Green, a Johns Hopkins University cryptographer and professor, welcomed the news, saying that ETSI's previous decision to keep its algorithms secret was out of touch. He likened it to serving formally dressed dinner guests a Jello salad.

“This whole idea of secret encryption algorithms is crazy, old-fashioned stuff. It’s very 1960s and 1970s and quaint,” he says. “If you’re not publishing [intentionally] weak algorithms, I don’t know why you would keep the algorithms secret.”

ETSI, which is based in France, was hit with intense criticism in July after Dutch researchers — Carlo Meijer, Wouter Bokslag, and Jos Wetzels of the Dutch cybersecurity consultancy Midnight Blue — found major flaws in four algorithms the standards body had created in the 90s to secure radios used by police, military and critical infrastructure around the world.

ETSI had kept the cryptographic algorithms secret for more than twenty-five years, carefully controlling who got to examine them and requiring a signed NDA from anyone ETSI did let view them. This prevented independent security experts from examining the algorithms for vulnerabilities.

The Dutch researchers bypassed this restriction by extracting the four algorithms from a Motorola radio they purchased online and reverse-engineering them. They found numerous critical flaws in the algorithms that would allow adversaries to intercept radio communications, decrypt them and even alter and spoof them. The flaws included what the researchers describe as an intentional backdoor — a purposely weakened algorithm — designed, presumably, to make it easier for parties who know about the flaw to intercept and decrypt radio communications. You can read details about the flaws in this story I wrote for WIRED in July

In an interview I conducted at the time with Brian Murgatroyd, chair of the technical body at ETSI responsible for developing the TETRA standard and algorithms, he revealed that the group had intentionally weakened that algorithm as a condition of export.

“[W]e would have preferred to have as strong a key as possible in all respects. But that just wasn’t possible because of the need for exportability,” Murgatroyd said. He revealed that prior to developing the algorithms, ETSI consulted with the UK government, who made “strong recommendations” that ETSI keep the algorithms secret.

This meant, however, that customers who purchased radio equipment from Airbus, Motorola, Damm, Hytera and others that use the algorithms weren’t aware of the flaws.

The algorithm with the backdoor is used primarily by critical infrastructure to secure data and commands in pipelines, railways, and the electric grid, including at least two dozen critical infrastructures in the US. Among them are electric utilities, a state border control agency, an oil refinery, chemical plants, an East Coast mass transit system, and three international airports, and a US Army training base.

The algorithm is also used by some police agencies and military around the world. Publicly, the algorithm with the backdoor is advertised as using a key with 80 bits of entropy, but the researchers found that it contained a secret feature that reduces it to just 32 bits of entropy. The researchers were able to crack the key in less than a minute using a standard laptop.

Malicious actors who crack the key would be able to snoop on police communications or intercept critical infrastructure communications to study how these systems work. And they could also potentially inject commands to the radios to trigger blackouts, halt gas pipeline flows, or re-route trains.

The researchers found another flaw in the standard itself that would allow similar decryption capabilities in TETRA-based radio systems sold only to police, prisons, military, intelligence agencies, and emergency services. Exploiting the flaw would let someone not only decrypt communications but also potentially send fraudulent messages to police, fire brigades, military troops and others to spread misinformation or direct the movement of personnel.

By the time the researchers discovered the flaws, ETSI was already three years into a project to replace the 1990s algorithms with new ones. After the researchers reported the flaws in the old algorithms to ETSI, the standards group incorporated changes into the new algorithms to address them.

“There were three mitigations that were necessary as a result of the researchers’ work, and we’re very grateful for that, because they showed us three vulnerabilities that we weren’t really aware of,” Murgatroyd told me.

He acknowledged the value in having independent experts outside of ETSI examine the algorithms for flaws, but insisted in July that the new algorithms would be kept secret like the old ones, despite the fact that this secrecy had prevented ETSI from learning about and fixing flaws in the old algorithms.

Here’s Murgatroyd’s comments at the time.

KZ: Who’s requiring that the algorithms be kept secret? Who’s making that decision?

BM: I wouldn’t say requiring; it’s a strong recommendation — from governments.

KZ: ETSI is keeping the algorithms secret because the government requested it?

BM: Because some of the algorithms involve critical national security, in terms of public safety.

KZ: But, as the researchers point out, an algorithm should be secure whether or not it’s public. It shouldn’t base its security on being kept secret.

BM: Yeah. I don’t know quite what the answer is. The fact is that these were private, and the fact is the new ones are also private. So that’s the state-of-play at the moment. Whether that changes in the future I don’t know.

KZ: If you’re saying that the only reason they’re secret is because the government has advised it, can ETSI decide on its own to make them public?

BM: I’d have to say yes.

KZ: So why don’t you?

BM: I don’t know.

KZ: Have there been any discussions in ETSI about making them public? Creating an algorithm a quarter of a century ago and keeping it secret might have been the right thing to do in 1995, but is it the right thing to do in 2023?

BM: Well I think that might be the basis of a discussion within ETSI. I’m not sure that anything is going to change that quickly. When we went to the ETSI board to form the new special committee to develop these [new] algorithms, it was explained then that [these algorithms] would be secret on the grounds of national security. And the board accepted that.

KZ: There was no pushback.

BM: Not that I’m aware of.

KZ: Is there any discussion going forward about at least bringing in independent researchers to do

> full analysis, with the understanding that the findings they uncover can be made public? You could fix the problems they encounter, and after they've reviewed your fixes, they can make their findings public, while the algorithms remain secret.
>
> **BM:** That would have been a great idea with the researchers this time. But they decided to release the algorithms as well [in addition to their findings]. But yeah scrutiny is very important.… I can't see anything wrong with what you just said, apart from the fact that we'd rather if someone came in to do an independent review of the algorithms … that they wouldn't then go and just give the information out.

That exchange brought heavy criticism from the security community, customers, and even some of its own members. Members who previously opposed making the old algorithms public have begun to reconsider that stance for the new algorithms.

Notably, ETSI announced recently that it had been hacked. The intruders used an unpatched vulnerability in its members-only web portal to access a database containing information about members. ETSI said it had engaged the French National Cybersecurity Agency to investigate the breach, but no further details were provided.

Boyer told me the attack did not damage the IT system and ETSI had fixed the vulnerability and "undertaken additional security actions and significantly strengthened its IT security procedures."

She said ETSI does not know who was behind the breach.

Wetzels, who was among those criticizing ETSI after his team discovered the vulnerabilities in the 90's algorithms, says that making the new algorithms public would be a "welcome development and a serious change in attitude from ETSI that would go a long way in making amends for the damage done by secret algorithms in multiple standards through the years."

ETSI has about 900 members around the world, which include governmental bodies, telecoms, tech companies and hardware manufacturers, network operators, research bodies, academics and others, according to its web site. Only a very small subset of these belong to the TETRA group and will have the ability to decide whether the new TETRA algorithms will remain secret or be made public.

15.Quantum Computing Review Q3 2023

by IDQ
https://www.idquantique.com/quantum-computing-review-q3-2023/?utm_term=quantum-computing-review-q3-2023&utm_campaign=&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_--_-quantum-computing-review-q3-2023

In this edition, we have some ground-breaking news from tech giants Google and IBM, plus a number of exciting collaborations between industry and academia, designed to expand the frontiers of quantum technologies. There is also news of poneering use of quantum computing in fields as diverse as chemical dynamics, particle physics and driverless cars!

Google's quantum breakthrough

Q3 got off to a rapid start with Google's quantum computing department announcing a major breakthrough on their quantum journey. In early July, researchers published a paper featuring their new 70 qubit system – a significant uplift in power over the previous 53 qubit system that demonstrated quantum supremacy back in 2019.

The exponential increase in power reportedly makes calculations almost instantly that conventional supercomputers would take 47 years to complete. Though the specific task the computer was asked to complete has little or no real-world applications, it serves to demonstrate the evolving potential of quantum computing systems.

IBM makes error correction simpler

In mid-August, researchers at IBM quantum published a new set of codes that effectively work with ten times fewer qubits; bringing practical, fault-tolerant quantum computing one step closer.

One of the biggest challenges to today's quantum computers is that they are "noisy". They have a high error rate that is a barrier to adoption.

However, advances in error correction, in tandem with hardware and processor innovation, are cause for optimism amongst the quantum computing community that fault tolerant quantum computing isn't just viable, but ultimately practical.

A new approach to quantum repeaters

Quantum networks won't work the same way as today's classical data networks. Quantum signals are more fragile by nature and next-generation networks will need to feature quantum repeaters.

A new Princeton study details the basis for a new approach to building quantum repeaters, combining significant advancements in photonic design and materials science.

Contemporary repeaters emit light in the visible spectrum, which degrades quickly over optical fiber and requires conversion before it can travel any significant distance. The new approach emits light at an infrared wavelength and doesn't require conversion, paving the way to simpler, more robust networks.

Legislative landscape

As the global race for quantum advantage continues, the Biden administration took steps to limit overseas investment by US entities in China, Hong Kong, and Macau. Specifically, an Executive Order published in August seeks to prohibit US investment in what it refers to as "national Security Technologies" most notably semiconductors, quantum technologies and artificial intelligence.

Quantum announcements

At the Quantum World Congress in Washington in September, IonQ announced an expansion of its product line with two new, rack-mounted processors: IonQ Forte Enterprise and IonQ Tempo. Both represent efforts by IonQ to reduce the overall footprint of its technology, making it more suitable for inclusion in conventional data centres. At the same time, IonQ announced it had been awarded an additional $25million contract to provide quantum computers to the US Air Force.

It's been a busy few months for IonQ, who also partnered with the University of Maryland in the development of the $20million National Quantum Laboratory (QLab), opened in September at the UMDs headquarters.

In a further example of commerce and academia collaborating on quantum, Abu Dhabi University and Vernewell Group signed a memorandum of understanding, signifying their intent to exploit the opportunities represented by DARQ technologies – Distributed Ledger, Artificial Intelligence, Extended Reality and

Quantum computing.

In August, Deutsche Telekom opened a Quantum Lab at its T-Lab facility in Berlin. Dedicated to quantum research and the integration of quantum technologies into commercial communications networks, the facility is connected to academic institutes in Berlin, Dresden, and Munich.

China Mobile collaborated with China Electronics Technology Group Corp (CETGC) to launch the largest quantum cloud computing platform in China. A hybrid environment, the cloud platform links classical computing resources with advanced 20-qubit quantum devices to provide an open testbed to researchers and enterprises, and to grant public access to universities and other agencies.

In the UK, Imperial College London launched its QuEST initiative (Centre for Quantum Engineering, Science and Technology). Designed to complement the UK Government's National Quantum Strategy, QuEST will provide further impetus to an already impressive legacy of quantum achievements at the world-famous institution.

In late July, D-Wave announced two new collaborations with the Institute of Quantum computing at the University of Waterloo. Funded by the Natural Sciences and Engineering Research Council, the long-term projects will focus on "identifying improvements in device design and materials quality that support increasingly coherent superconducting quantum processors".

Quantum applications

As quantum technology evolves, it is finding new applications across a wide range of disciplines. In the world of chemistry, researchers have used a trapped-ion quantum computer to revolutionize how we observe a geometric process in chemical dynamics that has had chemists and physicists stumped since the 1950s. In a paper published in Nature, they revealed how they designed and mapped the complex problem onto a small quantum device and slowed the process by a factor of 100 million.

In the field of Lidar applications and driverless cars, quantum technologies are being used to improve visibility of objects in bright sunlight. Driverless cars can use laser pulses to sense objects and measure how far away they are, but this can be affected in very bright conditions, or where light is reflected from nearby objects. Swapping out the lasers for particles of quantum light could make it easier for autonomous vehicles to avoid collisions.

In July, researchers from CERN, DESY, IBM Quantum and over 30 other organisations published a paper identifying specific activities in the realm of particle physics where emerging quantum computing technologies could be applied.

Quantum computing is very promising, but not every problem in particle physics is suited to this mode of computing. […]

> *It's important to ensure that we are ready and that we can accurately identify the areas where these technologies have the potential to be most useful for our community.*

Alberto Di Meglio, head of the CERN Quantum Technology Initiative (CERN QTI)

A research team at Ecole Normale Supérieure de Lyon, CNRS recently developed a quantum radar that could significantly outperform existing systems based on classical approaches. Previous research had demonstrated that quantum correlations could make radar detection up to four times faster. Initial results show the microwave quantum radar developed by the researchers sped up radar detection by 20% compared to classical radars.

16.Japan Announces Installation of Second Quantum Computer

by Matt Swayne
https://thequantuminsider.com/2023/10/10/japan-announces-installation-of-second-quantum-computer/

Fujitsu and research institute Riken have unveiled Japan’s second quantum computer, boasting 64 qubits, as part of the global effort to make quantum computing practical, according to Reuters.

This milestone in quantum computing development will see Fujitsu and the state-backed Riken institute integrating their newly developed quantum computer with a 40 qubit quantum computer simulator, the news service reported. The primary aim of this integration is to tackle the persistent challenge of eliminating errors that have hampered the ability of quantum systems to provide accurate results.

Shintaro Sato, the head of Fujitsu’s quantum laboratory, emphasized the magnitude of the achievement while acknowledging the long road ahead.

“It’s kind of a first or second step, we still have a long way to go,” Sato told reporters.

Governments and leading tech companies such as IBM and Alphabet have been actively investing in quantum computing research. Reuters points out that these quantum machines hold the promise of outperforming the fastest supercomputers. IBM, for instance, made headlines last year with the launch of a 433 qubit quantum computer, showcasing the rapid advancement in quantum computing capabilities.

Quantum bits, or qubits, are the fundamental units of quantum computing and are integral to the extraordinary processing power of these machines, leveraging the principles of quantum mechanics.

Thee successful development of Japan’s second quantum computer represents a crucial step forward and adds another name among nations in the race to become global leaders in quantum technology.

17.Mathematician warns US spies may be weakening next-gen encryption

by Matthew Sparkes
https://www.newscientist.com/article/2396510-mathematician-warns-us-spies-may-be-weakening-next-gen-encryption/

Quantum computers may soon be able to crack encryption methods in use today, so plans are already under way to replace them with new, secure algorithms. Now it seems the US National Security Agency may be undermining that process.

A prominent cryptography expert has told New Scientist that a US spy agency could be weakening a new generation of algorithms designed to protect against hackers equipped with quantum computers.

Daniel Bernstein at the University of Illinois Chicago says that the US National Institute of Standards and

Technology (NIST) is deliberately obscuring the level of involvement the US National Security Agency (NSA) has in developing new encryption standards for “post-quantum cryptography” (PQC). He also believes that NIST has made errors – either accidental or deliberate – in calculations describing the security of the new standards. NIST denies the claims.

“NIST isn’t following procedures designed to stop NSA from weakening PQC,” says Bernstein. “People choosing cryptographic standards should be transparently and verifiably following clear public rules so that we don’t need to worry about their motivations. NIST promised transparency and then claimed it had shown all its work, but that claim simply isn’t true.”

The mathematical problems we use to protect data are practically impossible for even the largest supercomputers to crack today. But when quantum computers become reliable and powerful enough, they will be able to break them in moments.

18.Possible Quantum Decryption Breakthrough

by Brian Wang
https://www.nextbigfuture.com/2023/10/possible-quantum-decryptian-breakthrough.html

Researcher show that *n*-bit integers can be factorized by independently running a quantum circuit with orders of magnitude fewer qubits many times. It then use polynomial-time classical post-processing. The correctness of the algorithm relies on a number-theoretic heuristic assumption reminiscent of those used in subexponential classical factorization algorithms. It is currently not clear if the algorithm can lead to improved physical implementations in practice.

Shor’s celebrated algorithm allows to factorize *n*-bit integers using a quantum circuit of size O(*n*^2). For factoring to be feasible in practice, however, it is desirable to reduce this number further. Indeed, all else being equal, the fewer quantum gates there are in a circuit, the likelier it is that it can be implemented without noise and decoherence destroying the quantum effects. The new algorithm can be thought of as a multidimensional analogue of Shor’s algorithm. At the core of the algorithm is a quantum procedure.

Without full fault tolerance in quantum computers we will never practically get past 100 qubits but full fault tolerance will eventually open up the possibility of billions of qubits and beyond. In a Wright Brothers Kittyhawk moment for Quantum Computing, a fully fault-tolerant algorithm was executed on real qubits. They were only three qubits but this was never done on real qubits before.

If the new decryption algorithm is verified and we get fault tolerant qubits at scale, then all current internet and financial encryption would be broken. There are quantum computing resistant math for encoding that would not be vulnerable to quantum computers, but they will likely take a decade or more to implement. It will still take many years for fault tolerant quantum qubits to scale.

19.Quantum Proof of Work Consensus on Blockchain Explained

by LCX Team
https://www.lcx.com/quantum-proof-of-work-consensus-on-blockchain-explained/

As the world of cryptocurrencies continues to evolve, one significant concern looms over the horizon: the threat posed by quantum computers. With their unprecedented computational power, quantum computers have the potential to undermine the security of traditional cryptographic systems, including those used in blockchain networks. To counter this emerging threat, researchers and developers have been exploring quantum-proof solutions, such as the Quantum-Proof of Work (QPW) consensus. In this article, we will delve into the concept of QPW consensus and explore its role in safeguarding the future of blockchain technology.

Quantum-Proof of Work Consensus

Prior to delving into the specifics of Quantum-Proof of Work, it is essential to understand the potential impact of quantum computers on blockchain networks. Currently, the vast majority of blockchains rely on cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC) to secure transactions and guarantee the immutability of the distributed ledger. However, quantum computers are able to rapidly solve the mathematical problems that underpin these algorithms, making them vulnerable to attack. Recognizing this challenge, researchers have been striving to develop quantum-resistant alternatives to ensure the long-term viability of blockchain technology.

The Quantum-Proof-of-Work consensus is an innovative method designed to protect blockchain networks from quantum attacks. It integrates aspects of Proof of Work (PoW) consensus with quantum-resistant cryptographic techniques to maintain the security and integrity of blockchain transactions.

Key Components of Quantum-Proof of Work

Hash-Based Functions: QPW consensus relies on the utilization of hash-based functions, such as the Merkle Tree, that are resistant to quantum computing attacks. These functions are integral to the mining process and provide a foundation for achieving quantum resistance.

Quantum-Resistant Cryptography: In contrast to traditional cryptographic systems, quantum-proof consensus algorithms employ quantum-resistant cryptographic primitives. Examples include the use of lattice-based cryptography, code-based cryptography, and multivariate cryptography, which offer resilience against quantum algorithms.

Post-Quantum Digital Signatures: Digital signatures play a crucial role in verifying the authenticity and integrity of transactions within blockchain networks. Quantum-proof consensus algorithms utilize post-quantum digital signature schemes, such as XMSS (eXtended Merkle Signature Scheme) and SPHINCS (SPHINCS+), to ensure the robustness of signatures against quantum attacks.

Benefits of Quantum-Proof of Work

Enhanced Security: By integrating quantum-resistant cryptographic techniques, QPW consensus ensures that blockchain networks remain secure even in the face of quantum threats. This safeguards the confidentiality, integrity, and availability of transactions, promoting trust and confidence in the system.

Continuity and Compatibility: Quantum-Proof of Work Consensus can be implemented as an upgrade to existing blockchain protocols, making it backward-compatible with earlier versions. This feature allows for a smooth transition to quantum-resistant systems without disrupting established networks and their functionalities.

Decentralization: QPW consensus retains the decentralized nature of blockchain networks, as it operates on the familiar principles of Proof of Work. Miners contribute their computational power to secure the network and validate transactions, ensuring the democratic and distributed nature of the blockchain ecosystem.

Challenges and Considerations

While QPoW shows promise in addressing the quantum computing challenge, several considerations must be taken into account during its implementation:

Performance Impact: Quantum-resistant cryptographic algorithms tend to be more computationally intensive, which can impact the overall performance and scalability of blockchain networks. Striking a balance between security and performance is crucial.

Standardization: The standardization of quantum-resistant cryptographic algorithms and protocols is essential to ensure interoperability and widespread adoption. Collaborative efforts among industry stakeholders and researchers are necessary to develop universally accepted standards.

Conclusion

The advent of quantum computing poses a significant threat to the security of traditional blockchain systems. Quantum-Proof of Work (QPoW) consensus algorithms offer a promising solution to safeguard the integrity of transactions and data against the power of quantum adversaries. By implementing QPW consensus, blockchain networks can adapt to the quantum era, ensuring the continued security and longevity of decentralized systems. Embracing QPoW ensures the long-term viability and resilience of blockchain technology, paving the way for a quantum-secure future. As researchers and developers work together to refine and enhance quantum-resistant solutions, the future of blockchain technology remains bright and hopefully impervious to the threats posed by quantum computing.

20.Linux Foundation Announces OpenPubkey Open Source Cryptographic Protocol

by Eduard Kovacs
https://www.securityweek.com/linux-foundation-announces-openpubkey-open-source-cryptographic-protocol/

The Linux Foundation on Wednesday announced OpenPubkey, an open source cryptographic protocol that should help boost supply chain security.

OpenPubkey was developed as part of BastionZero’s zero trust infrastructure access product and is now being integrated with Docker.

OpenPubkey is designed to enable binding crypto keys to users and workloads by turning an OpenID Connect identity provider into a certificate authority. Its goal is to provide enhanced passwordless authentication.

“This new cryptographic protocol empowers developers to build out software supply chain or security applications. OpenPubkey augments OpenID Connect to enable workloads and users to sign artifacts under their OpenID identity,” the Linux Foundation explained.

“These keys can be used to cryptographically sign statements, enabling applications such as secure remote access or software supply chain security features such as signed builds, deployments, and code commits,” it added.

The project’s developers noted that OpenPubkey is compatible with existing OpenID providers, including Microsoft, Google, Okta, Keycloak and OneLogin, and it does not require any changes to the provider.

The GitHub page set up for OpenPubkey provides the reference implementation source code and additional information.

21.11 notable post-quantum cryptography initiatives launched in 2023

by Michael Hill
https://www.csoonline.com/article/654887/11-notable-post-quantum-cryptography-initiatives-launched-in-2023.html

The point at which quantum computers will be capable of breaking existing cryptographic algorithms -- known as "Q-Day" -- is approaching. It's a juncture that's been discussed for years, but with advancements in computing power, post-quantum threats are becoming very real. Some security experts believe Q-Day will occur within the next decade, potentially leaving all digital information vulnerable under current encryption protocols.

Post-quantum cryptography (PQC) is therefore high on the agenda as the security community works to understand, build, and implement cryptographic encryption that can withstand post-quantum threats and attacks of the future.

"PQC migration provides an opportunity to re-evaluate the larger cybersecurity landscape," Dylan Rudy, a lead scientist within Booz Allen's quantum sciences team, tells CSO. By integrating new PQC algorithms into a zero-trust architecture, cybersecurity infrastructure can be redesigned into a new crypto agility framework, he says.

"A redesign to these new agile security principals would allow system stakeholders to respond to new threats introduced by emerging technologies by investigating existing cryptographic assets, identifying new cryptographic threat surfaces, and integrating new cryptographic solutions.”

Here are 11 notable initiatives, programs, standards, and resources launched this year to help the creation/development of and migration to PQC.

IETF launches working group to coordinate quantum-resistant cryptographic protocols

In January, the Internet Engineering Task Force (IETF) launched the Post-Quantum Use In Protocols (PQUIP) working group **to coordinate the use of cryptographic protocols** that are not susceptible to large quantum computers. "The idea of the working group is to be a standing venue to discuss PQC from an operational and engineering side," said Sofia Celi, co-chair of PQUI. "It is also a venue of last resort to discuss PQC-related issues in IETF protocols that have no associated maintenance on other working groups that the IETF has.”

The IESG said the working group has been set up on an experimental basis, and in two years, it intends to review it for rechartering to continue or else closure. In August, the group published the Post-Quantum Cryptography for Engineers paper to provide an overview of the current threat landscape and the relevant algorithms designed to help prevent those threats.

UK publishes National Quantum Strategy to steer technical standards

In March, the UK government published a new National Quantum Strategy detailing its 10-year plan for leading a quantum-enabled economy, recognizing the importance of quantum technologies for the UK's security.

The UK will work with relevant global bodies to ensure that global quantum technical standards promote its prosperity and security interests, including accelerating the commercialization of quantum technologies and supporting the sector in the UK, outlined the strategy.

The UK will also work with key partners to scope and identify the best approach to coordinating national engagement in priority areas of quantum technical standards development. Relevant industry and academia will be engaged in these efforts to track priority standards activity, raise stakeholder awareness, and develop roadmaps to support UK engagement with quantum standards development, it added.

"There are a number of early quantum standardization activities taking place globally with significant focus on quantum-safe cryptography and quantum key distribution (QKD), with UK leadership in these areas," the strategy read.

QuSecure pioneers live satellite quantum-resilient cryptographic communications link through space

In March, quantum security vendor QuSecure claimed to have accomplished the first known live, end-to-end quantum-resilient cryptographic communications satellite link through space. It marked the first time US satellite data transmissions had been protected from classical and quantum decryption attacks using PQC, according to the company. The quantum-secure communication to space and back to Earth was made through a Starlink satellite working with a leading global system integrator (GSI) and security provider.

This is significant because data shared between satellites and ground stations travels through the air and traditionally has been vulnerable to theft, leaving satellite communications even more accessible than typical internet communications, the vendor said.

QuSecure, Accenture achieve successful multi-orbit data communications test secured with PQC

Later in the same month, QuSecure announced it had collaborated with Accenture to accomplish the **first successful multi-orbit data communications test secured with PQC**. This demonstrated that crypto-agility, successfully rotating to a less vulnerable algorithm, is real and possible, achieved through an Accenture-facilitated low earth orbit (LEO) data transmission, the vendor said.

Prior to this advancement, data from multi-orbit satellites could be collected and potentially broken by classical means and quantum computers with enough power, QuSecure added. The transmission included a switch over from LEO to a geosynchronous orbit (GEO) satellite and back down to earth, as a model for redundancy in the event of a breach, failure, or threat to satellites in a single orbit.

"As more organizations are increasingly relying on space technology to provide solutions, resiliency and more relevant information, security of those systems and the data is paramount," commented Paul Thomas, space innovation lead for technology innovation at Accenture.

NCCoE addresses preparing for the adoption of new PQC algorithms

In April, the US National Cybersecurity Council of Excellence (NCCoE), a collaboration of cybersecurity experts from the public and private sectors, released a draft publication addressing preparation for adopting new PQC algorithms. Migration to Post-Quantum Cryptography extended the typical message of urgency to plan for migration seen in federal mandates to members of the private sector.

NCCoE said it would be engaging with industry collaborators, regulated industry sectors, and the US government to bring awareness to the issues involved in migrating to post-quantum algorithms and to prepare the crypto community for migration.

PQShield supports PQC migration, advanced side-channel secured implementations

In May, PQC standards company PQShield signed a Memorandum of Understanding (MoU) with Tata Consultancy Services (TCS), a leading IT Services, consulting, and business solutions organization, to help clients transition to quantum-secure solutions. It also announced a collaboration with eShard, a side-channel analysis and testing tools provider, to further **accelerate advanced side-channel secured implementations of PQC** that are critical for high-security standards across industries.

"Quantum computers pose a particular threat to large organizations given the sprawling nature of their cryptographic infrastructure and their reliance on secure communications," said Ali El Kaafarani, CEO and founder of PQShield. "We're seeing a significant shift in the commercial landscape as more of these businesses wake up to the urgency of the problem and seek out a solution."

X9 announces initiative to create PQC assessment guidelines

In June, the Accredited Standards Committee X9 Inc. (X9) announced a new initiative to create PQC assessment guidelines to act as a roadmap for PQC transitions. It invited participants to take part in the effort. When completed, the X9 guidelines might be used by an organization as a self-assessment tool, as an informal assessment of a third-party service provider, or as an independent assessment by a qualified information security professional, X9 said. An auditor or regulator might also refer to the assessment guidelines which could form a foundation for crypto agility standardization, it added.

"It will be important to have PQC assessment guidelines available before transitions are underway, for consistency to make the process as smooth as possible and the outcomes optimal," said Michael Talley, chair of the X9F1 Cryptographic Tools working group.

Google readies Chrome for future attacks with quantum-resistant encryption

In August, Google announced it was taking a major step in making web browsing safe from future quantum computers by adding Chrome support for quantum-resistant encryption. Dubbed **X25519Kyber768, the new quantum-resistant cryptography** will be a hybrid mechanism that combines the output of two cryptographic algorithms to encrypt Transport Layer Security (TLS) sessions.

These are X25519, an elliptic curve algorithm widely used for key agreement in TLS today, and Kyber-768, a quantum-resistant Key Encapsulation Method (KEM). The new hybrid encryption has been made available in Chrome 116, and behind a flag in Chrome 115.

"Google's announcement of shielding encryption keys in Chrome from quantum computers is very forward-looking," said Pareekh Jain, chief analyst at Pareekh Consulting. "Quantum computers' serious adoption is a few years away, but messages have a risk of getting stored now and decrypting later."

NIST publishes draft PQC standards for global framework

In August, the US National Institute of Standards and Technology (NIST) published draft PQC standards designed to form a future global framework to help organizations protect themselves from quantum-enabled cyberattacks.

The standards were selected by NIST following a seven-year process which began when the agency issued a public call for submissions to the PQC Standardization Process. NIST called for public feedback on three draft Federal Information Processing Standards (FIPS), which are based upon previously selected encryption algorithms.

The public-key encapsulation mechanism selected was CRYSTALS-KYBER, along with three digital signature schemes: CRYSTALS-Dilithium, FALCON, and SPHINCS+. It is intended that these algorithms will be capable of protecting sensitive US government information well into the foreseeable future, including after the advent of quantum computers, incorporated into three FIPS: FIPS 203, FIPS 204, and FIPS 205, NIST said.

CISA, NSA, NIST issue PQC migration resource

In August, the US Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and NIST published a factsheet on the impacts of quantum capabilities. It urged all organizations, especially those that support critical infrastructure, to begin early planning for migration to PQC standards by developing their own quantum-readiness roadmap.

Quantum-Readiness: Migration to Post-Quantum Cryptography outlined how organizations can prepare a cryptographic inventory, engage with technology vendors, and assess their supply chain reliance on quantum-vulnerable cryptography in systems and assets. The factsheet also provides recommendations for technology vendors whose products support the use of quantum-vulnerable cryptography.

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

Tech community launches PQC Coalition to drive understanding, adoption

In September, a community of technologists, researchers, and expert practitioners launched the PQC Coalition to drive progre ss toward broader understanding and public adoption of PQC algorithms. Founding coalition members include IBM Quantum, Microsoft, MITRE, PQShield, SandboxAQ, and the University of Waterloo.

The PQC Coalition will apply its collective technical expertise and influence to facilitate global adoption of PQC in commercial and open-source technologies. Coalition members will contribute their expertise to motivate and advance interoperable standards and technical approaches and step forward as knowledgeable experts in providing critical outreach and education.

The coalition will initially focus on four workstreams:

- Advancing standards relevant to PQC migration.
- Creating technical materials to support education and workforce development.
- Producing and verifying open-source, production-quality code, and implementing side-channel resistant code for industry verticals.
- Ensuring cryptographic agility.

22.Encryption services are sending the right message to the quantum code-breakers

by John Naughton
https://www.theguardian.com/commentisfree/2023/oct/07/encryption-services-quantum-computers-cryptography-rsa-signal-whatsapp

A spectre is haunting our networked world. It's the prospect of quantum computers. These are machines that harness some of the weirder properties of subatomic particles in ways that would make them exponentially more powerful than the computers we use today.

Existing computers are based on manipulating digital bits that can be either 1 (on) or 0 (off). Quantum machines, in contrast, work with qubits, which can be on and off simultaneously. (And, yes, I know that seems nuts, but then so does much of subatomic physics to the average layperson.) Such machines are fiendishly difficult to build, but about 80 or so small-scale ones already exist, with qubit counts ranging from five to 400. So that looming spectral presence is beginning to put on weight. And if researchers find a way of reliably scaling up these machines, then we will have moved into uncharted territory.

Why? Basically, because we have become a networked species, and as our lives and industries have moved online, all of our communications have become vulnerable to surveillance and manipulation by bad actors, public and private. To counter that, we have developed end-to-end encryption systems for making our communications – whether personal or commercial – more secure.

The key tool for providing that protection is a technology called public-key cryptography. It was originally conceived by British engineer and cryptographer James Ellis at GCHQ in 1970, but only broke into the public domain in 1976, when his US counterparts Whitfield Diffie and Martin Hellman came up with a practical method for establishing a shared key over an open communications channel without using a previously shared secret code. This approach was then formalised by three Massachusetts Institute of Technology scientists, Ronald Rivest, Adi Shamir and Leonard Adleman, and became the RSA algorithm (based on the first letters of their respective surnames).

Public-key systems work on what mathematicians call "one-way functions". For RSA, it's multiplication. It's easy to multiply numbers, but hard to factorise them. And if the individual numbers are very large prime numbers, then deducing the two factors that produced them rapidly becomes *very* difficult. In the RSA system, the big number becomes an individual's public key, which they can release to anyone (for example, in an email footer), and one of the primes becomes their private key. Anyone who wishes to communicate securely with them encrypts their message using the public key. But because only the recipient knows the private key, decryption is easy.

In practical encryption systems (such as the ones that secure Signal, Telegram, WhatsApp, iMessage, etc), all this stuff happens invisibly, through computation. What makes it secure is that the public key is, to all intents and purposes, uncrackable by brute-force computing. One estimate I've seen of how long it would take a 2019-era supercomputer to break a 256-bit key runs into trillions of years!

So essentially the security of our networked world rests on the inability of computers to break the encryption systems we use. For a long time, that was a comforting thought. But the advent of quantum computing has somewhat undermined such complacency. A large quantum machine may make light work of a task that defeats even a conventional supercomputer. Worse still, it's possible that some bad actors are already hoarding encrypted messages in anticipation of being able to break them when a suitable quantum machine arrives.

A pressing question, then, is when that moment may arrive. At present, nobody really knows. It's a bit like nuclear fusion. Quantum evangelists claim that it's only a few years away. At the high end, some observers think it's 30-plus years away and there are sceptics who find the whole idea implausible. But then it's not that long since people thought that large language models were pie in the sky. So it may be prudent not to be too complacent.

That's certainly the view taken by Signal, one of the providers of the encrypted messaging service that I and many of my colleagues use. "We are not in a position to judge which timeline is most likely," says a recent post on the Signal blog, "but we do see a real and growing risk which means we need to take steps today to address the future possibility of a large enough quantum computer being created."

The folks at Signal are taking one of the four post-quantum cryptography algorithms that have been chosen by the US National Institute of Standards and Technology to withstand attacks by quantum computers, but instead of using it to replace their existing public-key encryption system, they are layering the new algorithm on top of what they already have. "We are augmenting our existing cryptosystems," they say, "such that an attacker must break both systems in order to compute the keys protecting people's communications." And they will be rolling out this augmented system to all users in the next few months.

23.NTT DATA publishes a white paper summarizing points to remember when migrating to Post-Quantum Cryptography (PQC)

by NTT DATA Group Corporation

https://www.nttdata.com/global/en/news/press-release/2023/october/ntt-data-publishes-a-white-paper-summarizing-points-to-remember-when-migrating-to-pqc

NTT DATA, a global digital business and IT services provider, has published a white paper which has summarized points to remember when migrating existing cryptographic technologies used in various information infrastructures to Post-Quantum Cryptography (PQC).

Recently, there have been a number of announcements regarding the development, operation, and commercialization of quantum computers, and the day when quantum computers will be used in daily life is drawing near.
While quantum computers are expected to have faster processing speeds that far exceed those of supercomputers, they also carry the risk of making it easier to decipher encrypted data that is currently considered difficult to decipher, and preparations for their widespread use are progressing in countries around the world.

NTT DATA has been conducting research and development on quantum computers from both offensive and defensive aspects of utilization and security. This paper summarizes the latest trends in PQC and points to remember when migrating to a secure information infrastructure.

Background

The practical application of quantum computers is expected to accelerate advances in various fields such as materials development, medicine, finance, logistics, and AI, and improve the convenience of society and life. On the other hand, from the perspective of "cryptographic technologies" which are widely established in society as a whole, mainly in the financial field, there are concerns that quantum computers will be able to decipher existing encrypted data. In anticipation of these times, "Store now, decrypt later attack"*1 is beginning to be seen as a threat, in which attackers collect encrypted data over a long period of time now and attempt to decrypt it in the future when the performance of quantum computers has improved.

Against this background, the U.S. National Institute of Standards and Technology (NIST) estimates appearing the quantum computers capable of breaking RSA cryptosystems with the key length of 2048 bits by around 2030, and is proceeding with the standardization of Post-Quantum Cryptography (PQC). NIST decided on four public-key cryptographic algorithms as PQC in July 2022, and is expected to establish them as FIPS*2 standardization documents by 2024. Additionally, NIST has begun additional public applications for digital signatures category, continuing to standardize PQC.

Overview of the white paper

In this white paper, firstly we will introduce the PQC standardization at NIST, from its beginnings to the latest trends. Next, we summarize the following seven points to remember when migrating public-key cryptographic algorithms embedded in the information infrastructure of IT systems to PQC.

- Data size may increase
- Processing speed may be slow
- Increase crypto-agility
- Consider re-encrypting if encrypted data is stored in the system
- If using TLS hardware, is there enough time for procurement?
- Continuous collection of information published by NIST, SOG-IS, etc.
- Understand the PQC functions provided by the cloud service provider

Furthermore, we define the migration process to PQC and provide an overview of it.

White Paper

"Towards migration to secure information infrastructures even in quantum computers era"

About the future

NTT DATA will continue to accurately understand the PQC standardization activities in NIST. Based on this information, we will work with our customers to resolve issues when migrating their IT system to PQC. Through these activities, we aim to become a partner trusted by our customers over the long term.

Note

- Also called "Capture now, decrypt later attack" or "Harvest now, decrypt later attack”.

- FIPS is an abbreviation for Federal Information Processing Standards. FIPS is a set of standards and guidelines for computer systems established by NIST in the United States based on the Federal Information Security Management Act (FISMA).

- Crypto-Agility is a concept proposed by NIST. It refers to various improvements in design, implementation, and operation that allow the conventional encryption method used in an IT system to be quickly switched to another encryption method when it is compromised.
- SOG-IS is an abbreviation for Senior Officials Group Information Systems Security, and is a group that manages mutual recognition agreements among multiple countries in Europe. The SOG-IS Crypto Working Group has updated guidance documents on cryptographic algorithms, key lengths, and expiration dates almost every two years since 2016.

24.Researchers Test Undersea UK-Ireland Quantum Communications Link

by Matt Swayne
https://thequantuminsider.com/2023/10/05/researchers-test-undersea-uk-ireland-quantum-communications-link/

Researchers have successfully tested a fibre-optic cable to pass quantum communications under the Irish Sea between the Republic of Ireland and England.

It is the longest stretch of fibre-optic cable ever used to enable quantum communications underwater, and the first time a quantum link has ever been tested between Ireland and the UK.

The research team, led by Professor Marco Lucamarini from the University of York's Institute for Safe Autonomy, ran a series of experiments using a network cable named Rockabill.

This network, owned and operated by bandwidth infrastructure provider, euNetworks, is one of the newest commercial optical fibre systems in operation and connects Ireland to the United Kingdom, running 224 kilometres between Portrane in Ireland and Southport in the UK.

Overcoming limitations

Quantum communications operates on the principle that particles of light can transmit data along optical cables in a highly fragile state, which means that the particles collapse if interfered with by someone trying to manipulate or steal private data, such as bank information, in transit.

Professor Marco Lucamarini, from the University of York's Institute for Safe Autonomy, said: "Many large companies and organisations are interested in quantum communications to secure their data, but it has limitations, in particular the distance it can travel.

"The longer the distance, the more likely it is that photons – the particles of light that we use as carriers of quantum information – are lost, absorbed or scattered in the channel, which reduces the chances of the information reaching its target.

"This presents a problem when organisations need to send private information to other countries, where the additional challenge could be an ocean between the communications' start and end point."

Unique system

To overcome this limitation, the researchers exploited a new and unique underwater cable system between England and Ireland, reducing the chances of the quantum information being lost, allowing the particles that enter the link to reach the other end of the communication channel.

The same link also has very little time delay, which means a fast connection in sending and receiving data, which is crucial for financial transactions for example.

Professor Lucamarini said: “This is a truly exciting step forward in realising the full potential of quantum communications and for the future of securing private data in an environment that is shaping the so-called “quantum internet”.

“This project also advances the real-world integration of quantum communication technology into existing global telecommunications and network infrastructure – taking it out of the lab into a ‘real-world’ scenario.”

Detectors

The success of the experiments was largely due to highly sensitive detectors deployed at the Southport endpoint of the cable to reduce environmental – or ‘noise’ – interference.

Researchers liken this to interference from the sun on a laptop screen – reduce the external light interference and the user can function as normal again.

Paula Cogan, Chief Executive Officer of euNetworks, said: “We are proud to support a critical project that pushes the boundaries of quantum technology and has implications for the future of network security.

“The successful integration of quantum technology over commercial-grade optical fibre infrastructure at this distance is an exciting step forward. Rockabill, and the euNetworks’ Super Highway network it is part of, provide the ideal platform for new and progressive technologies that will enhance and innovate future network infrastructure.”

More experiments will need to be carried out using the same cable line to pave the way for integrating the services offered by quantum technologies into standard communications for industries sending private data between the UK and Ireland.

25.Quantum communication breakthrough: goes subsea, international

by Peter Clarke
https://www.eenewseurope.com/en/quantum-communication-breakthrough-goes-subsea-international/

Researchers have demonstrated quantum communications can be achieved over a sub-sea optical fibre cable between the United Kingdom and the Republic of Ireland.

The team, led by Professor Marco Lucamarini from the University of York, ran a series of experiments over a cable that runs between Portrane and Southport. Until now, no quantum link has ever been established between the two countries, nor on a span stretching this length on a subsea fibre optic cable, according to euNetworks Fiber UK Ltd. which operates the 224km Rockabill subsea network.

The successful demonstration between the UK and Ireland pushes the boundaries of quantum communications and the security of data from eavesdropping.

The research team from the University of York worked in collaboration with the Quantum Communications Hub of the ESPRC and euNetworks.

Quantum communication operates on the principle that particles of light can transmit data along optical cables in a highly fragile state. But the particles collapse if interfered with by someone trying to manipulate or steal private data, such as bank information, in transit.

“Many large companies and organisations are interested in quantum communications to secure their data, but it has limitations, particularly the distance it can travel,” said Professor Marco Lucamarini, in a statement issued by euNetworks and the University of York. “The longer the distance, the more likely it is that the photon – the particles of light that we use as carriers of quantum information – are lost, absorbed or scattered in the channel, which reduces the chances of the information reaching its target. This presents a problem when organisations need to send private digital information to other cities or other countries, where the additional challenge could also be an ocean between the communications’ start and end point.”

Special cable

The Rockabill subsea cable was key to the research. It provides an ultra-low loss fiber optic subsea cable with low latency, low attenuation and spans the 224 kilometers between Southport and Portrane without amplification or repeaters.

Both single and entangled photons were transported in the experiments the optical phase measured for use in twin-field and continuous-variable Quantum Key Distribution (QKD). The success of the experiments was largely due to highly sensitive detectors deployed at the Southport endpoint of the cable to reduce environmental noise levels.

Professor Lucamarini said: “This project also advances the real-world integration of quantum communication technology into existing global telecommunications and network infrastructure – taking it out of the lab into a ‘real-world’ scenario.”

More experiments are scheduled to be carried out using the same cable to prepare for the offering of quantum security on standard communications for those sending data between the UK and Ireland.

The project is due to be presented at the NATO Symposium on Quantum Technology for Defence and Security in Amsterdam on October 3.