Crypto News

Compiled by
Dhananjoy Dey
IIIT Lucknow
Chak Ganjaria, C. G. City
Lucknow – 226 002
email: dhananjoy.dey@gov.in

March 1, 2021

Contents

February 2021

28 Feb 2021

1 Intel Calls Silicon 'Greatest Weapon Against Security Threats'

by Tobias Mann

https://www.sdxcentral.com/articles/news/intel-calls-silicon-greatest-weapon-against-security-threats/2021/02/

Security rooted in silicon has the greatest opportunity to subvert both current and future threats, according to Martin Dixon, VP of security architecture and engineering at Intel.

In a recent blog post, Dixon broke down how Intel integrates security insights into its silicon to protect workloads from threats over the life of its products.

In the wake of side-channel attacks like Meltdown and Specter, silicon-layer security has become a hot topic, especially in the cloud where confidential computing is taking off.

In response, chipmakers have taken steps to make it easier for software vendors to secure their workloads. This can be done by accelerating stronger cryptographic algorithms or providing a secure enclave for the user's most sensitive data.

Last October, Intel revealed that its upcoming Ice Lake-based Xeon Scalable processors would feature secure enclaves, full memory encryption, firmware protections, and enhanced cryptographic performance compared to previous generation Xeons.

"The primary way attackers get into systems continues to be through something they can scale – and that is software," Dixon wrote. "By building silicon enhancements realized through logic inside of the processor," it's possible to eliminate performance overheads that might have dissuaded developers from implementing stronger encryption, he explained.

However, it's not just about making it easier to encrypt data at rest or in transit. One of the biggest challenges that silicon-based security is attempting to solve is how to encrypt data in use. This is exactly what the Linux Foundation's Confidential Computing Consortium, of which Intel is a member, is attempting to address.

By encrypting data in use, it can be processed in memory without being exposed to the rest of the system. This is especially important for organizations that handle sensitive data such as personally identifiable information, financial data, or health information, and thus need to mitigate threats that target the confidentiality and integrity of the applications and data in system memory.

Built With Purpose

According to Dixon, before Intel can integrate security features into its chips, the company has to understand where the threats are coming from.

"Our products are highly complex, and we cannot anticipate the myriad ways in which they will be used, nor how sophisticated third parties will seek to undermine their integrity," he wrote.

So Intel works with security researchers working in every environment their chips may find a home to identify, test, and validate the security capabilities of its products. It's about building a culture in which security concerns raised by the community are taken seriously and addressed quickly, Dixon explained.

And this culture extends into the development of new security capabilities. “The entirety of a product’s life needs to be secure, and our development practices stem from a security development lifecycle,” he wrote.

This lifecycle defines a set of processes that ensures that security principles and privacy tenants are considered at every step of product development. “Building security and privacy into products from concept to retirement is not only a strong development practice but it is also essential to enabling customers to truly unleash the power of their data,” Dixon wrote.

And with a few notable exceptions, Intel’s security philosophy appears to be paying off. “In 2020, 92% of vulnerabilities addressed in our products were a direct result of the proactive investment in our processes,” Dixon wrote.

Silicon Security Takes Off

And while Intel is heavily invested in silicon security, it’s hardly the only vendor doing it. Over the past year, every major chipmaker, including AMD and Nvidia, have made commitments to strengthening their hardware security capabilities.

All three companies are members of the Confidential Computing Consortium. Meanwhile, cloud providers, hyperscalers, and software vendors like VMware have steadily announced support for hardware-level security.

Early last year, Microsoft Azure and IBM launched confidential computing virtual machines (VMs) using Intel’s security capabilities. Meanwhile, Google and VMware tapped AMD for their own spin on the concept.

Both of Google Cloud’s Confidential VMs and Assured Workloads for government platforms, announced last summer, are based on security capabilities baked into AMD’s EPYC processors. And in an update to its popular vSphere platform, VMware added support for AMD’s secure encrypted virtualization-encrypted state function to enable memory encryption on the platform.

2 the growing need of ethical guidelines for quantum computing

by Apoorva Komarraju

https://www.analyticsinsight.net/the-growing-need-of-ethical-guidelines-for-quantum-computing/

The invention of supercomputers was a boon and a bane. Boon, because it started technological advancements that were once unimaginable and bane because it came with its own set of challenges, especially for ethical decision makers.

Supercomputers can perform insanely fast computing functions compared to normal desktop computers. They can breakdown codes, hack other systems, passwords, and that’s the problem. When you are online banking, you input all your valuable information. Considering the power of supercomputers, quantum computing can create problems.

Quantum Computing is thousand times faster than a regular computer

It uses four state qubits instead of the traditional two state transistors which enables greater computing ability and allows someone who knows quantum computing have a significant advantage over rest of the people who operate regular computers. Quantum computing can have a revolutionary impact on the human society, national security, global well-being, and commercial application across many industries. With the adoption of the quantum computing ecosystem around the world, several ethical questions have arisen among experts.

At present, we can compare the availability of quantum computers and how they will be used when they are developed. Right now, supercomputers are considered ethically wrong since its code states that every country needs to have the same amount of access to them.

The Opportunity

The technology is in its intermediate stage, so this is the time to consider its ethical implications. While this discussion is one of the hot topics of the tech world, it is important to note that ethical guidelines, of any sort, don't exist in the world as of yet. From the learnings of ethical principles and rules of other disruptive technologies like artificial intelligence, nanotech, nuclear energy, etc. there is a rising need to study the ethical implication, cautiously. Risks of quantum computing can be contained through effective governance and policy measures while spreading the right awareness. Developing effective guidelines of quantum computing for public and private sectors, education institutes, and other stakeholders is imperative to promote responsible quantum computing.

This ideology is bringing researchers and industry experts together for a discussion. Experts from public sector, private sector, academic sector, and civil society are stressing on the need to formulate guidelines and create an ethical framework for responsible and positive design and adoption of quantum computing technologies that can do good to society.

World Economic Forum is taking the following approach for this ethical conundrum:

- Frame stakeholder conversations and create an ecosystem awareness about how quantum ethics can be used for societal good.
- Study the native risks, important ethical questions, societal implications, and other unknown impacts of quantum computing.
- Design a thorough quantum computing ethics principles
- Design an extensive framework for correct design and adoption of responsible quantum computing
- Finally, test the framework in a couple of emerging programs of quantum computing which will be evaluated by a community of experts.

Like every technology in the world, misuse is a risk that the world is not ready for. Just like impossible technology predictions, there can be impossible consequences to technologies that we cannot predict. The pressing concern for researchers is to formulate guidelines as quickly as they can to avoid any chaos.

27 Feb 2021

3 cloud computing is the inevitable future of data analytics

by Apoorva Komarraju

https://www.analyticsinsight.net/cloud-computing-is-the-inevitable-future-of-data-analytics/

Companies of all sizes are onboarding the cloud to efficiently run their processes. They're being challenged to keep pace with enormous piles of data that can have an impact on business decisions. Differing analytics tools and unclear roles and functions are preventing organizations from making faster and better business decisions. This is the reason cloud-based analytic platforms are upping their game. The potential of cloud analytics is making technology leaders invest heavily and enjoy the benefits in the digital transformation space.

Cloud-based analytics help businesses become more competitive as they deliver data and analytical results to the end-users, giving them a chance to make smarter decisions. This has revolutionized big data and business intelligence. Via this technology, data flooding from various digital applications can be easily collected and analyzed.

Moving Data Analytics to The Cloud

Cloud technology is tailor-made for data analytics. Cloud-native applications have faster time-to-value implications leading to digital transformation. Until a few years ago, companies used to make their infrastructures to accommodate heavy demands. But eventually, the infrequent running of huge analytic workloads made having a flexible computing resource to manage costs, essential. Now, many service providers are offering cloud analytics to companies, fusing an agent or a script into the code that transfers information to the servers for data analysis. It enables marketing departments to attract the audience, improve websites, and create personalized content for the target audience. Apart from this, it also allows businesses to understand their demand and supply dynamics and predict consumer behavior.

Capabilities of The Cloud

The cloud not only provides readymade infrastructure but also the ability to alter the infrastructure quickly for companies to manage their fluctuating traffic. With cloud computing, organizations can include data storage and data analysis capacity to bring changes to the business. A company can quickly increase its cloud storage when the business grows or decrease it when the business slows down, which is cost-effective as compared to buying new hardware each time. It allows a company to be responsive to dynamic market demands and adjust its analytics capacity to meet customer needs and take advantage of every opportunity.

In-house analytics solutions can be expensive for businesses, cloud analytics, on the other hand, does not require any hardware, on-premises equipment, data centres or continuous upgrades. This means businesses can cut a lot of costs and have a flexible budget with simple subscriptions.

Companies have already begun combining data analytics and machine learning technologies to the cloud to evade any obstacles that can be faced while improving data quality. While this can reap benefits to any industry, organizations need to understand that poor data quality will lead to an undermined result of data analytics. Organizations that want to excel in becoming data-enabled are investing their focus towards improving the capabilities within the growth of cloud analytics. Successful processing of data

faster with the help of skilled professionals and the right management can result in the manifestation of AI assistants and improved chatbots which will increase the overall output of an organization.

26 Feb 2021

4 Qubit breakthrough is a big step towards networked quantum computers say researchers

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/qubit-breakthrough-is-a-big-step-towards-networked-quantum-computers-say-researchers/

Scientists have succeeded for the first time in entangling two separate qubits by connecting them via a cable, in a breakthrough that will likely accelerate the creation of quantum networks – which, by combining the capabilities of several quantum devices, could boost the potential of the technology even in its current limited state.

The researchers, from the University of Chicago's Cleland Lab, created two quantum nodes, themselves containing three superconducting qubits each. Using a one-meter-long superconducting cable to connect the nodes, the scientists then chose one qubit in each node and entangled them together by sending so-called "entangled quantum states" through the cable.

Taking the form of microwave photons, these entangled quantum states are extremely fragile, which makes the process particularly challenging; but the researchers nevertheless managed to transfer the entanglement from one node to the other, linking the qubits into a special quantum state that is still both fascinating and confounding to quantum scientists.

Qubits, or quantum bits, are the basic unit of quantum information, and their properties can be exploited to create next-generation quantum technologies; one of those properties is entanglement. Entanglement happens when two qubits are made to interact in a certain way, and they become inexplicably linked. Once entangled, they start sharing the same properties, no matter how distant they are from each other.

This means that by looking at one half of an entangled pair, scientists can know the properties of the other particle, even if they are thousands of kilometers away. Using entanglement, scientists could create webs of linked qubits, which could in turn help make quantum computing more powerful, as well as lay the groundwork for future quantum communication networks.

"Developing methods that allow us to transfer entangled states will be essential to scaling quantum computing," said Andrew Cleland, professor at the University of Chicago, who led the research.

For entanglement to be useful, it has to be established in the first place – something that is easier said than done. Within the Cleland Lab scientists' two-node experimental set-up, entanglement was transferred from node to cable to node in only a few tens of nanoseconds. With a nanosecond representing just one billionth of a second, the achievement was widely hailed as a successful one.

Quantum scientists around the world are actively working on different ways to establish entanglement between two qubits, but the most common procedure so far has consisted of creating a pair of entangled particles, and then distributing them between two points.

For example, once they are entangled, qubits can travel through networks of optical fiber. Last year, in

fact, another group of researchers from the University of Chicago used an existing underground network of optical fiber to support entangled photons travelling across a 52-mile network in the city's suburbs.

Another method consists of using satellites as a source of entangled photons, which allows the particles to travel over much longer distances. China is leading in this space: in 2017, the country's satellite Micius successfully delivered entangled particles to ground stations up to 1200 kilometers away.

Transferring entanglement from one qubit to another one located in another quantum node, however, is an unprecedented experiment. It doesn't stop here: once the Cleland Lab researchers used the cable to entangle two qubits in each of the two nodes, they then managed to extend this entanglement to the other qubits in each node.

In other words, Cleland and his team "amplified" the entanglement of qubits, until all six qubits in the two nodes were entangled in a single globally entangled state. The next challenge? To expand the system to three nodes, to build three-way entanglement.

By building up this small-scale network of entangled particles, the scientists are getting closer to establishing a quantum network that could have big implications for quantum computing. Entanglement could effectively be used to create quantum clusters, made up of linked qubits located in different quantum devices.

Much like supercomputers today carry out parallel calculations on many CPUs connected to one another, it is widely expected that in the future, quantum computing will be enabled by many different modules of such entangled qubits, all connected to each other to run a computation. "These modules will need to send complex quantum states to each other, and this is a big step towards that," said Cleland.

The quantum computers currently developed by tech giants the likes of IBM and Google can only support less than 100 qubits – nowhere near enough for the technology to start having a real-world impact. The companies are confident that quantum computers will scale up sooner rather than later; but a quantum network could, in principle, start showing results before a fully-fledged quantum computer sees the light of day.

In effect, by linking together quantum devices that, as they stand, have limited capabilities, scientists expect that they could create a quantum supercomputer more powerful than a quantum device operating on its own.

In addition to advancing quantum computing, a network of interlinked qubits could also enable new applications in the realm of quantum communications. The US and Chinese governments, as well as the EU, have all shown a marked interest in developing a quantum internet in recent years, which will rely on entanglement to exchange quantum information between quantum devices. One of the key applications of such a quantum network would be quantum key distribution – an un-hackable cryptography protocol that, once more, relies on inter-linked quantum particles.

25 Feb 2021

5 Taiwanese scholar enters semifinals in post-quantum cryptography competition

by Sophia Yang

https://www.taiwannews.com.tw/en/news/4135997

A four-year contest to find an international cryptographic standard is nearing its final stage, and a Taiwanese team has made it into the semi-finals, with the winner expected to be announced in 2022.

Deemed a potentially disruptive technology to revolutionize the future, the post-quantum cryptography market is estimated to reach US$214 million by 2025.

Maryland-based National Institute of Standards and Technology (NIST) began hosting the competition in 2016. The contest is set to select the winning system as the American national standard that will likely be accepted by the world.

Out of the original pool of 82 teams, two teams, led by Academia Sinica researchers Chou Tung and Yang Bo-ying, made it into the quarterfinals, showing Taiwan's strong presence in cryptography and growth momentum in the coming post-quantum era.

Chou, who is an assistant research fellow at a unit dedicated to advancing information technology, told Liberty Times that cryptography protects sensitive information to ensure cybersecurity and that public-key cryptography is already widely used.

However, there is an urgent need to develop a more secure method of public-key cryptography to resist the growing number of attacks by quantum computers, he said.

Chou's team is working on an encrypting system based on the classic McEliece scheme to effectively prevent cyberattacks during data transmissions.

24 Feb 2021

6 Raman Research Institute Achieves Breakthrough In Quantum Communication

by Shraddha Goled

https://analyticsindiamag.com/raman-research-institute-achieves-breakthrough-in-quantum-communication/

A team of researchers from the Raman Research Institute (RRI), Bangalore, demonstrated the transfer of a quantum distribution key between two buildings using an atmospheric channel. This is the first instance where the underlying technique – entanglement-based quantum-key distribution – has been demonstrated between ground stations (buildings) separated by 50m.

The team said this breakthrough has the potential to revolutionise cybersecurity in critical sectors such as banking and defence.

Prof Urbasi Sinha, who also heads RRI's Quantum Information and Computing (QuIC) lab, led the experiment. Prof Sinha said, "This is the country's first free-space quantum key distribution experiment. This experiment can be done and demonstrated only during the night." She said the atmospheric channel based experiment would further the Indian government's endeavour to connect different nodes in the country through free space and fibre-based channels and build a secure quantum-based communication network.

The team said leveraging this capability can help detect unauthorised break-in immediately and protect encrypted information from threats that might arise from future computational advances.

7 Quantum shuttle to quantum processor made in Germany launched

by Forschungszentrum Juelich

https://phys.org/news/2021-02-quantum-shuttle-processor-germany.html

The quantum computer race is in full swing. Germany has long been one of the world leaders in basic research. An alliance between Forschungszentrum Jülich and the semiconductor manufacturer Infinion, together with institutes of the Fraunhofer-Gesellschaft (IAF, IPMS) as well as the Leibniz Association (IHP, IKZ), the universities of Regensburg and Konstanz and the quantum start-up HQS, now aims to apply the results to industrial production. The goal is a semiconductor quantum processor made in Germany that is based on the "shuttling" of electrons and is to be achieved with technology available in Germany. The QUASAR project, which is funded with over 7.5 million euros by the Federal Ministry of Education and Research (BMBF), aims to lay the foundations for the industrial production of quantum processors over the next four years.

Quantum computers have the potential to outperform conventional supercomputers by far in certain problems, for example when it comes to controlling traffic flows in metropolitan areas or simulating materials at the atomic level. But it is still unclear which approach will win the race among quantum computers. Experiments with superconducting qubits, the smallest units of a quantum computer, are currently the most advanced. For example, Google's quantum chips and the experimental quantum computer in the European Quantum Flagship project, which is to go into operation this year at Forschungszentrum Jülich, are based on them. But when it comes to large numbers of qubits, semiconductor qubits may have the advantage.

"At Jülich, we are investigating both types of qubits, semiconductor-based and superconductor-based. There are strong synergy effects, for example, in the development of quantum software, component development and their integration into experimental computer architectures," says Prof. Wolfgang Marquardt, Chairman of the Board of Directors of Forschungszentrum Jülich. "In the long term, we want to realize a freely accessible quantum computer for science at Jülich. The QUASAR project is an important step for this project – in combination with our other activities, such as the European Quantum Flagship or the research of quantum materials."

Silicon electron spin qubits are one promising system for semiconductor qubits because they have comparatively robust quantum properties and are much smaller in size than superconducting quantum bits. "A big advantage is that their production is largely compatible with the production of silicon processors. This means that, in principle, there is already a lot of experience with the fabrication processes," says project coordinator Professor Hendrik Bluhm, Director at the JARA Institute for Quantum Information at Forschungszentrum Jülich. One example is Infineon in Dresden: in the project, the German semiconductor manufacturer helps with its production expertise adapting the component design for industrial manufacturing.

"Fundamental questions still need to be clarified. So far, it has not been possible to scale up quantum chips as easily as conventional computer chips. One problem has been geometric constraints. The qubits usually have to be very close together in order for them to be coupled to each other. Therefore, semiconductor qubits have been demonstrated up to now primarily in components that have no more than two coupled qubits close to each other. For a scalable architecture, however, we need more space on the quantum chip, for example for feed lines and control electronics," says Hendrik Bluhm.

In order to increase the distances, the researchers from the JARA cooperation of Forschungszentrum

Jülich and RWTH Aachen University, together with other research partners, have developed a something called a quantum bus. This special interconnection element allows distances of up to 10 micrometers between the individual qubits to be bridged efficiently. In silicon qubits, the quantum information is encoded by the spin of electrons located in quantum dots – special nanoscopic semiconductor structures. The quantum bus can capture the electrons on these quantum dots and transport them in a controlled way without losing the quantum information.

From the laboratory to production

The exchange of electrons is also known as "shuttling". In the laboratory, experimental samples are already showing promising results. Now the Jülich researchers want to adapt the device's design to industrial manufacturing processes. To this end, they have joined forces in the QUASAR project with Infineon Dresden, the start-up HQS specializing in quantum mechanical material simulations, institutes of the Fraunhofer-Gesellschaft (IAF, IPMS) as well as the Leibniz Association (IHP, IKZ) and the universities in Regensburg and Konstanz.

"One of the challenges here is the required degree of material quality, which is much higher for this application than for the production of conventional computer chips," says Hendrik Bluhm. "Another open point is the miniaturization of the control systems on the chip. In principle, however, we see great potential in this approach for complex circuits. Millions of qubits are realistic."

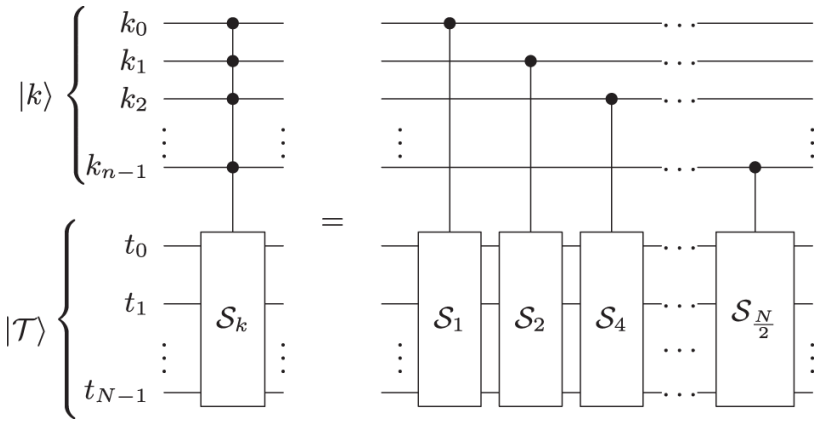
The QUASAR project will run until January 2025. The next step is to build a demonstrator with around 25 coupled qubits, which will be implemented in a follow-up project and integrated into the modular HPC environment of the Jülich Supercomputing Centre via the "Jülich User Infrastructure for Quantum Computing" (JUNIQ) with cloud access.

8 A quantum algorithm for string matching

https://www.swissquantumhub.com/a-quantum-algorithm-for-string-matching/

Algorithms that search for a pattern within a larger data-set appear ubiquitously in text and image processing.

Pattern matching algorithms are used ubiquitously used in image processing, the study of DNA sequences, and data compression and statistics, to name a few. Thus, accelerating pattern matching using a quantum computer would be a boon to all these areas.



Researchers at Joint Quantum Institute, NIST/University of Maryland and IonQ have developed an explicit, circuit-level implementation of a quantum pattern-matching algorithm that matches a search string (pattern) of length M inside a longer text of length N.

Their algorithm has a time complexity of $O(\sqrt{N})$ while the space complexity remains modest at $O(N + M)$.

They also reported the quantum gate counts relevant for both pre-fault-tolerant and fault-tolerant regimes.

23 Feb 2021

9 A quantum computer just solved a decades-old problem three million times faster than a classical computer

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/a-quantum-computer-just-solved-a-decades-old-problem-three-million-times-faster-than-a-classical-computer/

Scientists from quantum computing company D-Wave have demonstrated that, using a method called quantum annealing, they could simulate some materials up to three million times faster than it would take with corresponding classical methods.

Together with researchers from Google, the scientists set out to measure the speed of simulation in one of D-Wave's quantum annealing processors, and found that performance increased with both simulation size and problem difficulty, to reach a million-fold speedup over what could be achieved with a classical CPU.

The calculation that D-Wave and Google's teams tackled is a real-world problem; in fact, it has already been resolved by the 2016 winners of the Nobel Prize in Physics, Vadim Berezinskii, J. Michael Kosterlitz and David Thouless, who studied the behavior of so-called "**exotic magnetism**", which occurs in quantum magnetic systems.

The Nobel Prize winners used advanced mathematical methods to describe, in the 1970s, the properties of a two-dimensional quantum magnet, which shed light on the strange – or "exotic" – states that matter can take on.

Instead of proving quantum supremacy, which happens when a quantum computer runs a calculation that is impossible to resolve with classical means, D-Wave's latest research demonstrates that the company's quantum annealing processors can lead to a computational performance advantage.

"This work is the clearest evidence yet that quantum effects provide a computational advantage in D-Wave processors," said Andrew King, director of performance research at D-Wave.

D-Wave's processors are based on quantum annealing technology, which is a quantum computing technique used to find solutions to optimization problems. While some argue that the scope of the problems that can be resolved by the technology is limited, quantum annealing processors are easier to control and operate than their gate-based equivalents, which is why D-Wave's technology has already reached much higher numbers of qubits than can be found in the devices built by big players like IBM or Google.

To simulate exotic magnetism, King and his team used the D-Wave 2,000-qubit system, which was recently revised to reduce noise, to model a programmable quantum magnetic system, just like Berezinskii,

Kosterlitz and Thouless did in the 1970s to observe the unusual states of matter. The researchers also programmed a standard classical algorithm for this kind of simulation, called a "path-integral Monte Carlo" (PIMC), to compare the quantum results with CPU-run calculations. As the numbers show, the quantum simulation outperformed classical methods by a margin.

"What we see is a huge benefit in absolute terms," said King. "This simulation is a real problem that scientists have already attacked using the algorithms we compared against, marking a significant milestone and an important foundation for future development. This wouldn't have been possible today without D-Wave's lower noise processor."

Equally as significant as the performance milestone, said D-Wave's team, is the fact that the quantum annealing processors were used to run a practical application, instead of a proof-of-concept or an engineered, synthetic problem with little real-world relevance. Until now, quantum methods have mostly been leveraged to prove that the technology has the potential to solve practical problems, and is yet to make tangible marks in the real world.

In contrast, D-Wave's latest experiment resolved a meaningful problem that scientists are interested in independent of quantum computing. The findings have already attracted the attention of scientists around the world.

"The search for quantum advantage in computations is becoming increasingly lively because there are special problems where genuine progress is being made. These problems may appear somewhat contrived even to physicists," said Gabriel Aeppli, professor of physics at ETH Zürich and EPF Lausanne.

"But in this paper from a collaboration between D-Wave Systems, Google, and Simon Fraser University, it appears that there is an advantage for quantum annealing using a special purpose processor over classical simulations for the more 'practical' problem of finding the equilibrium state of a particular quantum magnet."

D-Wave, however, stayed clear of claiming quantum advantage, which happens when a quantum processor can demonstrate superiority over all possible classical competition; King stressed that it is still possible to design highly specialized algorithms to simulate the model once the properties of the model are already known.

The real significance of the experiment lies in the proof that a computational advantage can already be achieved using existing quantum methods to solve a valuable materials science problem.

"These experiments are an important advance in the field, providing the best look yet at the inner workings of D-Wave computers, and showing a scaling advantage over its chief classical competition," said King. "All quantum computing platforms will have to pass this kind of checkpoint on the way to widespread adoption."

Although D-Wave's 2000-qubit system was used for the research due to the technology's lower noise rates, the company recently released a 5000-qubit quantum processor, which is already available for programmers to build quantum applications.

From improving the logistics of retail supply chains to simulating new proteins for therapeutic drugs, through optimizing vehicles' routes through busy city streets, D-Wave is currently counting 250 early quantum annealing applications from various different customers.

22 Feb 2021

10 A speed limit also applies in the quantum world

https://www.swissquantumhub.com/a-speed-limit-also-applies-in-the-quantum-world/

Physicists at the University of Bonn have shown what the speed limit is for complex quantum operations. The fact that there is a speed limit in the microcosm was already theoretically demonstrated by two Soviet physicists, Leonid Mandelstam and Igor Tamm more than 60 years ago.

In their study, the researchers experimentally investigated exactly where this limit lies. They used a cesium atom and two laser beams perfectly superimposed but directed against each other as a tray. This superposition, called interference by physicists, creates a standing wave of light: a sequence of mountains and valleys that initially do not move.

In the case of the transport of an atom, for example, the deeper the valley into which the cesium atom is trapped, the more spread the energies of the quantum states in the valley are, and ultimately the faster the atom can be transported. The study shows that a lower speed limit applies to such processes than that predicted by the two Soviet physicists: It is determined not only by the energy uncertainty, but also by the number of intermediate states. In this way, the work improves the theoretical understanding of complex quantum processes and their constraints.

11 30,000 Macs infected with new Silver Sparrow malware

by Catalin Cimpanu

https://www.zdnet.com/article/30000-macs-infected-with-new-silver-sparrow-malware/

Security researchers have spotted a new malware operation targeting Mac devices that has silently infected almost 30,000 systems.

Named **Silver Sparrow**, the malware was discovered by security researchers from Red Canary and analyzed together with researchers from Malwarebytes and VMWare Carbon Black.

"According to data provided by Malwarebytes, Silver Sparrow had infected 29,139 macOS endpoints across 153 countries as of February 17, including high volumes of detection in the United States, the United Kingdom, Canada, France, and Germany," Red Canary's Tony Lambert wrote in a report published last week.

But despite the high number of infections, details about how the malware was distributed and infected users are still scarce, and it's unclear if Silver Sparrow was hidden inside malicious ads, pirated apps, or fake Flash updaters – the classic distribution vector for most Mac malware strains these days.

Furthermore, the purpose of this malware is also unclear, and researchers don't know what its final goal is.

Once Silver Sparrow infects a system, the malware just waits for new commands from its operators – commands that never arrived during the time researchers analyzed it, hoping to learn more of its inner workings prior to releasing their report.

But this shouldn't be interpreted as a failed malware strain, Red Canary warns. It may be possible that the malware is capable of detecting researchers analyzing its behavior and is simply avoiding delivering its second-stage payloads to these systems.

The large number of infected systems clearly suggests this is a very serious threat and not just some threat actor's one-off tests.

silver sparrow supports m1 chips

In addition, the malware also comes with support for infecting macOS systems running on Apple's latest M1 chip architecture, once again confirming this is a novel and well-maintained threat.

In fact, Silver Sparrow is the second malware strain discovered that can run on M1 architectures after the first was discovered just four days before, showing exactly how cutting-edge this new threat really is.

"Though we haven't observed Silver Sparrow delivering additional malicious payloads yet, its forward-looking M1 chip compatibility, global reach, relatively high infection rate, and operational maturity suggest Silver Sparrow is a reasonably serious threat, uniquely positioned to deliver a potentially impactful payload at a moment's notice," Lambert warned in his report.

"Given these causes for concern, in the spirit of transparency, we wanted to share everything we know with the broader infosec industry sooner rather than later."

The Red Canary report contains indicators of compromise, such as files and file paths created and used by the malware, which can be used to detect infected systems.

12 'Importance of cybersecurity still not well understood by all organisations': Cybersecurity Tech Accord

by Anuj Bhatia

https://indianexpress.com/article/technology/tech-news-technology/importance-of-cybersecurity-is-still-not-well-understood-by-all-organizations-cybersecurity-tech-accord-7

A study conducted by the Economic Intelligence Unit (EIU) and the Cybersecurity Tech Accord reveals that state-sponsored cyberattacks are a major concern for private organisations, which could not only dent their reputation but also hit them financially. The study highlights how the pandemic has increased some of the risks that could lead to malicious cyberattacks orchestrated by state-led actors on their organisations.

"The rise in state-sponsored cyberattacks targeting other governments, businesses and even private citizens is extremely concerning and requires a global response," Annalaura Gallo, Head of Secretariat, Cybersecurity Tech Accord, told Indianexpress.com in an email interview.

The Accord, which is a coalition of 150 companies, is the pact to jointly work together on cybersecurity issues. In 2018, a total of 34 big-tech companies including Facebook and Microsoft signed the Cybersecurity Tech Accord. Apple, Amazon and Alphabet are not part of the Cybersecurity Tech Accord.

The survey of more than 500 director-level executives from firms based in Asia-Pacific, Europe, and the United States with familiarity with their organisation's cybersecurity strategy found that state-led cyberattacks on their firms will only increase in the next five years. About 80% of the respondents, who took part in the survey conducted between November and December 2020, indicated that state-led and sponsored cyberattacks are a source of major concern for organisations.

The recent SolarWinds hack that affected over 250 federal agencies including the U.S. Treasury Department, State Department, and even top Fortune 500 companies like Microsoft, Cisco and Intel has shaken the cybersecurity world. Although the aftermath of the SolarWinds hack is yet to be evaluated, the breach posed a number of cybersecurity challenges that need to be addressed.

"At its core, these types of attacks illustrate why is it important that governments focus their attention on improving cyber defenses, but also agree on what actions should be prohibited online, and hold perpetrators accountable," says Gallo.

State-sponsored cyber attacks have increased manifold in recent years. In June last year, Australia's Prime Minister Scott Morrison held a press conference in which he revealed that the country was under a broad cyberattack from a "state-based actor" targeting government, public services and businesses. He declined to name the actor, but many speculated that the cyberattacks were part of Australia's rising rift with China.

Cyber attackers are not even sparing hospitals that are already under increased pressure amid rising coronavirus cases. Last month, hospitals in France were hit with ransomware attacks as the IT systems at three hospitals were affected.

What's important to note about the survey results is that 68% of executives feel their organisations are "very" or "completely" prepared to deal with a cyberattack. However, the report noted that while many companies feel prepared to handle state-sponsored attacks, the reality is indeed very different.

"It is true that the importance of cybersecurity is still not something that is well understood by all organisations," Gallo said. "We need to acknowledge that as in the offline world, there is no such thing as 100% security online. Organisations need to prioritise their investments and apply risk management principles to their overall security approaches,"

21 Feb 2021

13 Encrypted Quantum Computing: When Ignorance Is Wanted

by university of vienna

https://scitechdaily.com/encrypted-quantum-computing-when-ignorance-is-wanted/

Quantum computers promise not only to outperform classical machines in certain important tasks, but also to maintain the privacy of data processing. The secure delegation of computations has been an increasingly important issue since the possibility of utilizing cloud computing and cloud networks. Of particular interest is the ability to exploit quantum technology that allows for unconditional security, meaning that no assumptions about the computational power of a potential adversary need to be made.

Different quantum protocols have been proposed, all of which make trade-offs between computational performance, security, and resources. Classical protocols, for example, are either limited to trivial computations or are restricted in their security. In contrast, homomorphic quantum encryption is one of the most promising schemes for secure delegated computation. Here, the client's data is encrypted in such a way that the server can process it even though he cannot decrypt it. Moreover, opposed to other protocols, the client and server do not need to communicate during the computation which dramatically boosts the protocol's performance and practicality.

In an international collaboration led by Prof. Philip Walther from the University of Vienna scientists from Austria, Singapore and Italy teamed up to implement a new quantum computation protocol where the client has the option of encrypting his input data so that the computer cannot learn anything about them, yet can still perform the calculation. After the computation, the client can then decrypt the output data again to read out the result of the calculation. For the experimental demonstration, the team used

quantum light, which consists of individual photons, to implement this so-called homomorphic quantum encryption in a quantum walk process. Quantum walks are interesting special-purpose examples of quantum computation because they are hard for classical computers, whereas being feasible for single photons.

By combining an integrated photonic platform built at the Polytechnic University of Milan, together with a novel theoretical proposal developed at the Singapore University of Technology and Design, scientist from the University of Vienna demonstrated the security of the encrypted data and investigated the behavior increasing the complexity of the computations.

The team was able to show that the security of the encrypted data improves the larger the dimension of the quantum walk calculation becomes. Furthermore, recent theoretical work indicates that future experiments taking advantage of various photonic degrees of freedom would also contribute to an improvement in data security; one can anticipate further optimizations in the future. "Our results indicate that the level of security improves even further, when increasing the number of photons that carry the data," says Philip Walther and concludes "this is exciting and we anticipate further developments of secure quantum computing in the future."

19 Feb 2021

14 Linked Quantum Devices Called 'Big Step Forward' Toward Super-Secure Quantum Internet

by Matt Swayne

https://thequantumdaily.com/2021/02/19/linked-quantum-devices-called-big-step-forward-toward-super-secure-quantum-internet/

A team of researchers created a quantum Internet by linking three quantum devices together, Nature is reporting. In a world where billions of classical devices are linked together over the web, this may not sound like a major feat, but researchers are suggesting the team cleared a major hurdle toward a future quantum internet.

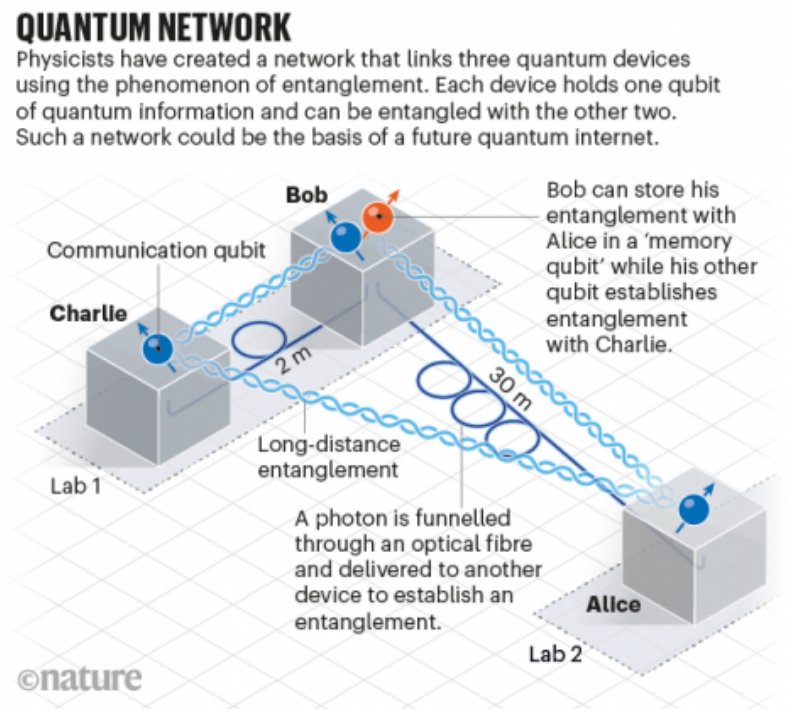
In a study, the research team led by physicist Ronald Hanson at the Delft University of Technology reported that they linked three devices together so that any two devices in the network ended up with mutually entangled qubits. The qubits were also placed in a three-way entangled state at all three devices, according to the team.

Hanson is a key figure in the emerging quantum industry, serving as QuTech's principal investigator. The company's website also reports he worked as its Scientific Director in 2016-2020. He currently chairs the steering board of Quantum Delta NL, the foundation responsible for the National Agenda Quantum Technology.

"It's a big step forward," Rodney Van Meter, a quantum-network engineer at Keio University in Tokyo, told Nature.

A quantum internet would enable ultrasecure communications. It could also pave the way for highly sensitive sensors and scientific equipment.

Quantum networks are so difficult to create because they rely on the super-sensitive realm of quantum physics. In the quantum world, elementary particles and atoms can exist in superposition – multiple simultaneous states – and they can be entangled with other particles, according to Nature. This gives



quantum computers their massive ability to perform calculations, but also make them susceptible to noise and errors.

The devices use a synthetic diamond crystal to store quantum information.

According to Nature, researchers can make the nitrogen qubit in these diamond devices emit a photon, which will be automatically entangled to the atom's state. The photon is then pushed into an optical fibre and to another device.

A three-node quantum network has been built before, Nature pointed out, but this approach seems better fit to create practical applications. However, those practical applications won't be ready immediately. The team said that more work needs to improve the system's performance.

In 2015, the team successfully entangled two diamond-based devices.

15 Physicists Propose a 'Force Field' to Protect Sensitive Quantum Computers From Noise

by mike mcrae

https://www.sciencealert.com/synthetic-magnetic-fields-could-help-protect-fragile-quantum-information

Creating a quantum computer requires an ability to stroke the edges of reality with the quietest of touches. Too much 'noise' and the delicate state of the system collapses, leaving you with a very expensive paperweight.

One way to reduce the risk of this occurring is to build in checks and balances that help to shield the blurred state of reality at the core of quantum computers – and now scientists have proposed a new way to do just that.

Theoretical physicists from RWTH Aachen University in Germany have proposed what's known as a 'synthetic magnetic field', which they think could help protect the fragile qubits needed in a quantum computer.

"We have designed a circuit composed of state-of-the-art superconducting circuit elements and a nonreciprocal device, that can be used to passively implement the GKP quantum error-correcting code," the team writes in their paper.

The basis for the design is a concept that's nearly 20 years old (we'll get to that in a moment), one that simply isn't feasible based on its requirement of impossibly strong magnetic fields. The new approach attempts to get around this issue.

Instead of the solid, bit-based language of 1s and 0s that informs the operations of your smartphone or desktop, quantum computing relies on a less binary, and far less definitive approach to crunching numbers.

Quantum bits, or qubits, are individual units of its language based on the probability of quantum mechanics. String enough together and their seemingly random tumbling sets the foundations for a different unique approach to problem solving.

A qubit is an odd creature though, something that has no real equivalent in our day-to-day experience. Unobserved, it could be simultaneously in the position of 1, 0, or both. But as soon as you look at it, the qubit settles into a single, more mundane state.

In physics, this act of looking doesn't even need to be an intentional stare. The buzz of electromagnetic radiation, a stray bump of a neighbouring particle... and that qubit can quickly find itself part of the scenery, losing its essential powers of probability.

This 'noise' only gets worse as we grow devices to include more qubits, something that is necessary to make quantum computers powerful enough to be capable of the high-level processing we expect of them.

A promising method for ensuring a qubit stays fuzzy long enough to be useful is to entangle it with other qubits located elsewhere, meaning its probabilities are now dependent on other, equally fuzzy particles sitting in zones unlikely to be slammed by the same noise.

If that's done right, engineers can ensure a level of quantum error correction – an insurance scheme that allows the qubit to cope with the occasional shake, rattle, and roll of surrounding noise.

And this is where we return to the new paper. Back in 2001, a trio of researchers – Daniel Gottesman, Alexeir Kitaev, and John Preskill – formulated a way to encode this kind of protection into a space as an intrinsic feature of the circuitry holding the qubits, potentially allowing for slimmer hardware.

It became known as the Gottesman-Kitaev-Preskill (GKP) code. There was just one problem – the GKP code relied on confining an electron to just two dimensions using intense, large magnetic fields in a way that just isn't practical. What's more, processes for detecting and recovering from errors are also fairly complicated, demanding even more chunks of hardware.

To really get the most out of the GKP code's benefits, quantum engineers would need a more passive, hands-off approach for shielding and recovering a qubit's information from noise.

So in this innovative new proposal, physicists suggest replacing the impossibly large magnetic field with a superconducting circuit comprising of components that serve much the same purpose, ironing out the noise.

The technicalities of the setup aren't for general reading, but Anja Metelmann at APS Physics does a top job of going through them step-by-step for those eager for details.

For it to work, there would need to be a way for photons – effectively ripples in the electromagnetic field that carry the electron's forces – to be manipulated by that very field. Given the photon's neutrality, this just isn't a possibility.

There is a workaround, though. In recent years physicists have found a way to control photons so they can be channelled like electrons, by manipulating the optics of a space so it takes on certain magnetic-like characteristics.

So-called synthetic magnetic fields permit photons to be directed, giving engineers a way to craft devices in which light waves can be forced to behave more like a current.

The new paper lays out a way to use this synthetic magnetic field to protect a theoretical single electron in a crystal, confined to a 2D plane. When they ran calculations to see how it would react when subjected to a strong, real magnetic field, which usually would interfere with the system, they showed that their new set-up could protect it.

"We find that the circuit is naturally protected against the common noise channels in superconducting circuits, such as charge and flux noise, implying that it can be used for passive quantum error correction," the team explains in their paper.

Before we get a working prototype of this quantum error-correcting machinery, there are plenty of kinks to work out experimentally. It's all good on paper, but left to be seen if the technology does cooperate as expected.

In time, we might have a relatively simple device that turns an impractical – but otherwise efficient – concept for scaling up quantum computers into a real possibility, opening the way for error tolerant technology that has until now been mostly theoretical.

16 Coding for Qubits: How to Program in Quantum Computer Assembly Language

by W. Wayt Gibbs

https://spectrum.ieee.org/tech-talk/computing/software/qscout-sandia-open-source-quantum-computer-and-jaqal-quantum-assembly-language

Quantum computing arguably isn't quite full-fledged computing till there's quantum software as well as hardware. One open-source quantum computer project at Sandia National Laboratories in Albuquerque, New Mexico aims to address this disparity with a custom-made assembly language for quantum computation.

Over the next several years, physicist Susan Clark and her team at Sandia plan to use a $25 million, 5-year grant they won from the U.S. Department of Energy to run code provided by academic, commercial, and independent researchers around the world on their "QSCOUT" platform as they steadily upgrade it from 3 qubits today to as many as 32 qubits by 2023.

QSCOUT stands for the Quantum Scientific Computing Open User Testbed and consists of ionized ytterbium atoms levitating inside a vacuum chamber. Flashes of ultraviolet laser light spin these atoms about, executing algorithms written in the team's fledgling quantum assembly code – which they've named Just Another Quantum Assembly Language or JAQAL. (They've in fact trademarked the name as Jaqal with lowercase letters "aqal," so all subsequent references will use that handle instead.)

Although Google, IBM, and some other companies have built bigger quantum machines and produced their own programming languages, Clark says that QSCOUT offers some advantages to those keen to explore this frontier of computer science. Superconducting gates, like those in the Google and IBM machines, are certainly fast. But they're also unstable, losing coherence (and data) in less than a second.

Thanks to ion-trapping technology similar to that developed by the company IonQ (which has published a nice explainer here), Clark says QSCOUT can maintain its computation's coherence – think of it like a computational equivalent of retaining a train of thought – over as much as 10 seconds. "That's the best out there," Clark says. "But our gates are a little slower."

The real advantage of QSCOUT is not performance, however, but the ability it gives users to control as much or as little of the computer's operation as they want to – even adding new or altered operations to the basic instruction set architecture of the machine. "QSCOUT is like a breadboard, while what companies are offering are like printed circuits," says Andrew Landahl, who leads the QSCOUT software team.

"Our users are scientists who want to do controlled experiments. When they ask for two quantum gates to happen at the same time, they mean it," he says. Commercial systems tend to optimize users' programs to improve their performance. "But they don't give you a lot of details of what's going on under the hood," Clark says. In these early days, when it is still so unclear how best to deal with major problems of noise, data persistence, and scalability, there's a role for a quantum machine that just does what you tell it to do.

To deliver that combination of precision and flexibility, Landahl says, they created Jaqal, which includes commands to initialize the ions as qubits, rotate them individually or together into various states, entangle them into superpositions, and read out their end states as output data. (See "A 'Hello World' Program in Jaqal," below.)

The first line of any Jaqal program, e.g.,

```
from qscout.v1.std usepulses *
```

loads a gate pulse file that defines the standard operations ("gates," in the lingo of quantum computing). This scheme allows for easy extensibility. Landahl says that the next version will add new instructions to support more than 10 qubits and add new functions. Plus, he says, users can even write their own functions, too.

One addition high on the wish list, Clark says, is a feature taken for granted in classical computing: the ability to do a partial measurement of a computation in progress and to then make adjustments based on the intermediate state. The interconnectedness of qubits makes such partial measurements tricky in the quantum realm, but experimentalists have shown it can be done.

Practical programs will intermix quantum and classical operations, so the QSCOUT team has also released on Github a Python package called JaqalPaq that provides a Jaqal emulator as well as commands to include Jaqal code as an object inside a larger Python program.

Most of the first five project proposals that Sandia accepted from an initial batch of 15 applicants will perform benchmarking of various kinds against other quantum computers. But, Clark says, "One of the teams [led by Phil Richerme at Indiana University, Bloomington] is solving a small quantum chemistry problem by finding the ground states of a particular molecule."

She says she plans to invite a second round of proposals in March, after the team has upgraded the

machine from 3 to 10 qubits.

A "Hello World" Program in Jaqal

One of the simplest non-trivial programs typically run on a new quantum computer, Landahl says, is code that entangles two qubits into one of the so-called Bell states, which are superpositions of the classical 0 and 1 binary states. The Jaqal documentation gives an example of a 15-line program that defines two textbook operations, executes those instructions to prepare a Bell state, and then reads out measurements of the two qubits' resulting states.

But as a trapped-ion computer, QSCOUT supports a nifty operation called a Mølmer-Sørensen gate that offers a shortcut. Exploiting that allows the 6-line program below to accomplish the same task – and to repeat it 1024 times:

```
register q[2]         // Define a 2-qubit register

loop 1024 {           // Sequential statements, repeated 1024x
    prepare_all      // Prepare each qubit in the |0⟩ state
    Sxx q[0] q[1]     // Perform the Mølmer-Sørensen gate
    measure_all      // Measure each qubit and output results
}
```

17 Microsoft says SolarWinds hackers stole source code for 3 products

by dan goodin

https://arstechnica.com/information-technology/2021/02/microsoft-says-solarwinds-hackers-stole-source-code-for-3-products/

The hackers behind one of the worst breaches in US history read and downloaded some Microsoft source code, but there's no evidence they were able to access production servers or customer data, Microsoft said on Thursday. The software maker also said it found no evidence the hackers used the Microsoft compromise to attack customers.

Microsoft released those findings after completing an investigation begun in December, after learning its network had been compromised. The breach was part of a wide-ranging hack that compromised the distribution system for the widely used Orion network-management software from SolarWinds and pushed out malicious updates to Microsoft and roughly 18,000 other customers.

The hackers then used the updates to compromise nine federal agencies and about 100 private-sector companies, the White House said on Wednesday. The federal government has said that the hackers were likely backed by the Kremlin.

In a post Thursday morning, Microsoft said it had completed its investigation into the hack of its network.

"Our analysis shows the first viewing of a file in a source repository was in late November and ended when we secured the affected accounts," Thursday's report stated. "We continued to see unsuccessful attempts at access by the actor into early January 2021, when the attempts stopped."

The vast majority of source code was never accessed, and for those repositories that were accessed, only a "few" individual files were viewed as a result of a repository search, the company said. There was no case in which all repositories for a given product or service were accessed, the company added.

For a "small" number of repositories, there was additional access, including the downloading of source code. Affected repositories contained source code for:

- a small subset of Azure components (subsets of service, security, identity)
- a small subset of Intune components
- a small subset of Exchange components

Thursday's report went on to say that, based on searches the hackers performed on repositories, their intent appeared to be uncovering "secrets" included in the source code.

"Our development policy prohibits secrets in code and we run automated tools to verify compliance," company officials wrote. "Because of the detected activity, we immediately initiated a verification process for current and historical branches of the repositories. We have confirmed that the repositories complied and did not contain any live, production credentials."

The hack campaign began no later than October 2019, when the attackers used the SolarWinds software build system in a test run. The campaign wasn't discovered until December 13, when security firm FireEye, itself a victim, first revealed the SolarWinds compromise and the resulting software supply chain attack on its customers. Other organizations hit included Malwarebytes, Mimecast, and the US departments of Energy, Commerce, Treasury, and Homeland Security.

17 Feb 2021

18 Machine learning blazes path to reliable near-term quantum computers

by Charles Poling

https://www.lanl.gov/discover/news-release-archive/2021/February/0217-machine-learning.php

Using machine learning to develop algorithms that compensate for the crippling noise endemic on today's quantum computers offers a way to maximize their power for reliably performing actual tasks, according to a new paper.

"The method, called noise-aware circuit learning, or NACL, will play an important role in the quest for quantum advantage, when a quantum computer solves a problem that's impossible on a classical computer," said Patrick Coles, a quantum physicist in at Los Alamos National Laboratory and lead author on the paper, "Machine learning of noise-resilient quantum circuits," published today in Physical Review X Quantum.

"Our work automates designing quantum computing algorithms and comes up with the fastest algorithm tailored to the imperfections of a specific hardware platform and a specific task," said Lukasz Cincio, a quantum physicist at Los Alamos. "This will be a crucial tool for using real quantum computers in the

near term for work such as simulating a biological molecule or physics simulations relevant to the national security mission at Los Alamos."

Coles likened the machine-learning approach to a vaccine that strengthens a person's resistance to a virus by training their immune system in the presence of a piece of that pathogen. Similarly, the machine learning trains quantum circuits in the presence of a specific quantum computer's noise processes. The resulting circuit, or algorithm, is resistant to that noise, which is the biggest problem facing today's noisy intermediate-scale quantum computers.

NACL starts with two things: a description of a computational task and a model of the noise on the quantum computer that will perform the task. Then the machine learning program formulates a circuit with the best strategy to run the task in the most reliable way on that particular computer, based on its unique noise profile.

The framework is practical, too. It works for all of the common tasks in quantum computing – extracting observables, preparing quantum states, and compiling circuits. The Los Alamos–led team tested sample problems in each of these areas and demonstrated that NACL reduces error rates in algorithms run on quantum computers by factors of 2 to 3 compared to textbook circuits for the same tasks.

Noise leads to errors

Errors are caused by disruptive noise in the form of various kinds of interactions between the quantum bits, or qubits, and the surrounding environment. Those interactions cause the qubits to lose their "quantumness" in a process called decoherence, which occurs within a millionth of a second.

Quantum bits are the fundamental processing unit of a quantum computer. Bits on a classical computer can only have a value of 0 or 1 – that's the basis of all computing on your phone or laptop. Qubits, on the other hand, can have a value of 0, 1, or various "superpositions" that result in probabilities between 0 and 1. That quality gives quantum computers their potential for supreme processing power.

Previous machine-learning attempts sought to reduce the errors by shortening the circuits and reducing the number of logic gates, but did not profile the errors in particular hardware platforms. Gates are the part of a circuit that act on the qubits as part of an algorithm. Previous machine-learning codes did not train to recognize and compensate for noise.

Letting the computer do the work

"In this new research, we let the computer discover what's best," Coles explained. "In essence, we say, 'Computer, please find the best strategy for making a resilient circuit.' We found the computer discovers strategies that make sense to us."

It turns out the shortest circuit isn't always the best. Every gate is imperfect, so sometimes it's better to add gates that correct errors on the fly.

For instance, if a particular computer erroneously over-rotates one individual qubit, the machine learning might surround it with other gates to correct errors from original gate. That's a well-known strategy called dynamically corrected gates, but it emerges spontaneously out of the NACL optimization procedure.

Another common error-correction strategy in quantum computing is called drift, or the do-nothing gate – a qubit is left undisturbed by the algorithm, and its quantum state drifts, like a boat on a lake. If its

state is a certain electron spin, for example, the earth's magnetic field might cause a tiny alteration in that spin. But NACL rarely chooses to let a qubit sit and do nothing – the machine learning wants a gate to do something.

Classical training, quantum results

Coles said the team's theoretical work involved developing a noise model of the quantum computer of interest, putting that model on a classical desktop computer, then training the machine learning on that model. After training, the machine learning output circuit, or algorithm, adapted to that particular quantum computer's noise model.

The team then transferred the resulting algorithm to the quantum computer and evaluated its outcomes on target problems. The evaluation is based on how closely the observed output matched standard ways of measuring that output for a known problem

NACL brings a few advantages compared to other methods of compiling circuits for qubits. For instance, NACL can automatically derive known noise suppression concepts and apply them where they are useful. It also incorporates common-sense strategies such as minimizing the number of noisy idle gates and maximizing the use of ideal gates.

"For the future, it will be important to figure out how to scale NACL to develop noise-resilient circuits for larger devices," Coles said.

19 Quantum Resistant Cryptography: Issues and Actions

by Ludovic Perret

https://observatoire-fic.com/cryptographie-resistante-au-quantique-enjeux-et-actions/

What would you say about a company whose 10-year strategic plans, exploration plans or R&D secrets that make up its industrial added value of tomorrow would be stolen today to be exploited in a few years without these actions? are detectable? You would certainly answer that at the very least the company has lost part of its value, if it has not already compromised its future.

What will you say in the near future, estimated at 5 to 10 years, about a company whose most valuable information is constantly and systematically vulnerable to attacks, and that in addition these attacks are undetectable? You will certainly answer that the survival of this company is threatened and that its CEOs and CIOs should have anticipated this threat and implemented appropriate countermeasures sufficiently early.

These two scenarios are not fictional scenarios; they correspond to the real threat posed by the future capacities of the quantum computer on our IT infrastructures and in particular on the resistance of traditional cryptographic protocols.

This article aims to clarify the nature and state of this quantum threat to cybersecurity, the advances made by institutions to standardize robust solutions to this threat, and the recommendations that can be made to help companies engage, starting today. 'hui', the implementation of protective countermeasures.

What predictions for the quantum computer?

"Quantum supremacy" or "quantum advantage" is a concept which designates the moment when the superiority of a quantum computer is demonstrated over the most advanced of classical "supercomputers". The 50 qubit threshold corresponds to the generally accepted limit of quantum supremacy.

In October 2019, Google announced that it had achieved this quantum supremacy; in September 2020, IBM announces in its roadmap a quantum computer of 1000 qubits in 2023; In December 2020, a team from the University of Science and Technology of China announced that it had significantly exceeded Google's results. Very recently, a team of researchers from Sorbonne University, CNRS and an American start-up QC Ware announced a quantum advantage. In practice, even if these announcements are still debated within the scientific community on their interpretation, they show very rapid and tangible progress towards a quantum computer with effective computing capacities.

What threats to infrastructure security?

In practice, the quantum computer is the promise of a machine that uses quantum physics phenomena to increase its computing power tenfold. The quantum computer thus makes it possible to solve certain mathematical problems much more efficiently than a conventional machine and this calls into question the security of the encryption algorithms used in cryptography.

Two types of cryptographic systems are commonly used.

(i) **Systems with private or symmetric keys are not threatened:** the same secret key is used to encrypt and decrypt messages, typically with the AES (Advanced Encryption Standard) algorithm. The quantum computer can speed up the search for the secret key, but doubling the size of the keys will simply prevent this threat.

(ii) **Public key or asymmetric key systems are threatened:** a public key is used to encrypt the message while a private key is used to decrypt the message.

Public key cryptography systems are based on mathematical problems that are complex to solve for the classical computer but easy to solve for the quantum computer.

- **RSA public key encryption** – named after its inventors R. Rivest, A. Shamir, L. Adelman Turing Prize in 2002 – is based on the difficulty of decomposing large numbers into products of prime factors.
- Diffie-Hellman key exchange is based on the difficulty of finding a discrete logarithm in finite fields or elliptic curves.

The security of a cryptosystem is measured by the complexity, or execution time, of the best attack against it. The security level is defined as the binary logarithm of the execution time of the best attack. For example, the RSA-1024 standard has an 80-bit security level. The best attack with conventional computers takes on the order of operations, or about 400 years. With access to a quantum machine, the security level of RSA or Diffie-Hellman goes to zero bits and therefore no longer guarantees any security.

A very frequent use case is the connection to a secure website: the public key system makes it possible to initiate and authenticate a transaction between your computer's browser and the website's server, and to exchange keys. private. These private keys will then be used to encrypt the entire transaction with a symmetric algorithm (because it is much faster). The questioning of the security of public key

systems therefore calls into question here the confidentiality of the private keys and therefore of all the data exchanged (personal data, banking, e-commerce, etc.).

In practice, public key cryptography is used almost everywhere and all communications that are secure today are impacted by the arrival of the quantum computer: communications over Internet networks (https, VPN IPSec), mobile messaging applications (Signal, WhatsApp ...), electronic signature protocols, blockchain applications ...

Why do we need to act today?

The NIST (National Institute of Standards and Technologies – US Agency of Commerce Department) had announced in 2016 that this threat would turn into reality by 2030. Some confusion or uncertainty still exists today among experts on this deadline (2025? 2030?). But, the NSA (National Security Agency – US) pointed out, as early as 2015, that the progress of the quantum computer had reached such a point that the risk could no longer be ignored and that organizations must, now, begin a transition. towards quantum resistant cryptography solutions. In particular, an official goal has been announced to switch US administrations to quantum-resistant cryptography as early as 2024 (M. Scholl, NIST, 2017).

In addition, we must realize that the threat is present today. Indeed, following the principle of "collect now and decrypt tomorrow" ("harvest now and decrypt later"), data can be captured and stored today by organizations with significant storage resources, to be decrypted and used tomorrow. .

All sectors of activity and all companies are affected and must act quickly. For sectors that manage long-lived secret and sensitive data such as defense, finance, aerospace, energy, automotive, pharmaceuticals, health, an urgent issue is already present.

In October 2018, research and consultancy firm Gartner ranked the quantum computer number one in the list of future IT upheavals for which CIOs are not well prepared.

What responses to this threat?

A first operational response is provided by "quantum-resistant cryptography" or "post-quantum cryptography". Indeed, a practical approach is to build cryptosystems with public keys, with other mathematical problems than the existing problems in threatened algorithms, and resistant to quantum. Quantum-resistant cryptography includes cryptography based on Euclidean networks, multivariate cryptography, cryptography based on error correcting codes, isogenies, and cryptography based on hash functions.

A second complementary answer is provided by "quantum cryptography" and in particular quantum key distribution (QKD for Quantum Key Distribution). The QKD, whose security is based on the laws of quantum physics, makes it possible to exchange a secret key which is then used to secure a conventional symmetric cryptography protocol. Some technological challenges still need to be resolved to manage long distances, for integration into telecommunications infrastructure, and on deployment costs.

To support and boost this transition, the President of the Republic Emmanuel Macron announced on January 21, 2021 the national investment plan in quantum. This plan aims to put France in the world's leading trio of quantum technologies; it includes an investment of 1.8 billion euros over 5 years, with a component of 150 million euros on quantum-resistant cryptography.

Which quantum resistant cryptography standards?

NIST launched an international call in 2016 to standardize quantum resistant algorithms. As a priority, NIST wants to have standards for two functionalities: digital signature and key exchange. NIST called on the global scientific community to submit its best algorithms and analyze the level of trust that can be attributed to them.

Eighty-four international research teams submitted their submissions from 26 countries (including thirteen teams with at least one French researcher). In 2020, the second selection round selected fifteen bids, with the prospect of a final decision in 2022.

From a scientific and technical point of view, these algorithms are more complex with characteristics very different from current standards and often longer keys; and this poses performance challenges depending on the expected objectives and the material or application environment. In practice, and depending on the use cases, different algorithms may be used. These differences are one reason which explains the very long selection time for algorithms standardized at NIST and makes the integration of new cryptosystems into existing applications more complex.

Finally, it is important to stress that China, still very active on quantum subjects, already concluded in January 2020 the selection phase of its new standards.

What technical solutions for quantum resistant cryptography?

Today, the NIST in the USA and the ANSSI (National Agency for the Security of Information Systems) in France advocate a hybrid approach that allows to keep the existing traditional cryptography layer, and just requires the integration of a additional layer of quantum resistant cryptography.

This strategy offers several advantages:

- The risk of migration is reduced because the existing layer is not called into question (there is no degradation of the existing security).
- Companies can more easily maintain their certifications on their products.
- The transition to quantum resistant cryptography can be done seamlessly.

CryptoNext Security is a startup resulting from French university research (CNRS, INRIA and Sorbonne University), whose founders participate in the NIST process with an algorithm in the final phase of the competition. CryptoNext Security now offers a hybrid library of quantum resistant cryptography, integrating all the final candidate algorithms of the NIST standardization process and responding to the main use cases.

What actions and which migration plans for companies?

The full deployment of a new cryptographic standard like AES (private key cryptography) took 20 years. Experts estimate at 10 years the minimum required for this work of migrating our public key infrastructure to quantum resistant algorithms.

For companies, the transition is a colossal challenge, a path strewn with pitfalls involving a multitude of systems and actors. But, the sooner the company invests and structures its approach to quantum-resistant cryptography, the sooner it will gain a competitive advantage over its competitors. And in practice, if the

threat appears to be an upheaval, the implementation of this transition should be addressed in a structured manner as part of a migration plan that is an integral part of the company's current cybersecurity plan.

Without waiting for the results of the NIST competition or, worse, a possible effective translation of the threat into a real attack (knowing that it is undetectable), every company can now get to work to establish a quantum transition plan. This transition plan must include the following components:

- The mapping of systems and applications that use cryptography, in particular, public key cryptography.
- The definition of a quantum resistant cryptography policy, time objectives, and a strategy to achieve these objectives.
- The definition of an action plan.

Naturally, this plan relating to the migration of cryptography solutions must be placed in parallel with a mapping of the most critical data making it possible to prioritize migration. This migration plan also questions stakeholders such as suppliers, their progress plans and the protection of their critical systems.

Transition actions may affect very sensitive areas in terms of sovereignty, security and performance such as payment systems or certain communications in aerospace or defense. The deployment of this new generation cryptography can have a significant impact on a company's IT infrastructure (size of keys, file format, etc.) and it is therefore necessary to carry out tests as soon as possible. The implementation of these actions will therefore naturally take time and must be strongly anticipated.

So that each company can initiate the process, two levers can be activated immediately:

(i) **Crypto-agility**

Today cryptography algorithms are often "hard" integrated into application code. Their change is therefore inflexible and very expensive. In a simplified manner, the choice of a cryptography algorithm must be made "configurable" and companies will obtain several benefits:

- **Anticipate:** this change can be organized now to allow a smooth evolution of cryptosystems afterwards according to the recommended standards.
- **Create technical flexibility to change algorithms** based on use cases, performance needs or to switch from one quantum resistant cryptography solution provider to another.
- **Create flexibility** to adapt to standards that may be different depending on the territory, for example in the USA and China.

(ii) **Commitment to projects on limited areas**

While the security of an infrastructure in the face of the quantum threat can naturally only be assessed as a whole, it seems essential to start migration projects now on limited perimeters of the company. This will make it possible to initiate and test the approach, but also and above all, to integrate and disseminate the challenges, culture and know-how of quantum-resistant cryptography in the teams.

Large organizations have already taken the plunge and initiated projects as part of their quantum plan. For example, for NATO, CryptoNext Security provides a well-known mobile messaging application, in which a quantum-resistant cryptography overlay has been embedded. With Thales, a partnership has

been established to integrate a quantum resistant cryptography option in the Luna HSMs (Hardware Security Modules); HSM being the heart of security infrastructure for many companies.

In conclusion, the US National Academy of Sciences effectively synthesized the challenges for companies in a study published in 2018: "Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough – and the time frame for transitioning to a new security protocol is sufficiently long and uncertain – that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster".

20 Will Quantum Computers Truly Serve Humanity?

by Ilyas Khan

https://www.scientificamerican.com/article/will-quantum-computers-truly-serve-humanity/

From the very earliest times in recorded human history, new technologies have been used for both positive and negative reasons.

Scientists such as Robert Oppenheimer, whose work ultimately led to the development of nuclear weapons, have been only too aware of how technology can be harnessed by society in ways that raise ethical challenges.

Our experience with computers is no different. New technologies have made life easier in many ways, yet we can see that when controls are lacking it can lead to unforeseen societal outcomes.

We are now on the threshold of a new computer technology era more powerful than anything that preceded it: the age of quantum computing. However, this time we have a chance to stop and think carefully about the ethical use of a transformative technology today while we can still shape the future.

Nicholas Niggli, deputy secretary general of the Republic and State of Geneva, a Swiss canton, believes it is possible to take a step back and anticipate the full breadth of the possible impact of new technologies. He cites the example of Henry Dunant, who co-founded the Red Cross. Dunant saw the impact of modern weaponry on war and conceived of the Geneva Convention as a way to instill rules designed to mitigate the new and fearsome development of mechanical warfare.

The word disruptive does not come close to describing the impact of quantum technologies. We have become used to describing new applications in sectors such as finance and banking as "disruptive," but this term is inadequate in the context of quantum computing. There is now an informed consensus that the impact of quantum computers across a whole swathe of humanity's lived experience will be akin to an industrial revolution at an even larger scale than anything we have previously experienced.

There exist today literally dozens of quantum processors all over the world with hundreds more likely to be unveiled this year and next. Many of these computers are still experimental, but companies such as IBM, Honeywell and Google have published roadmaps that will take today's early-stage devices to ones that will have real-world impact. There are also dozens of start-up companies all over the world who have raised capital to build a quantum computer, including IQM in Finland, OQC in the United Kingdom and Xanadu in North America.

Quantum computing will likely make its initial presence felt in areas such as drug development and discovery, materials science for developing better batteries, and carbon sequestration. It will also amplify

the power of AI in many fields, including real natural language processing and "optimization" problems, for example, efficiently routing thousands of delivery vans. Certain uses of quantum computers are already entering real life. The generation of unhackable keys for cybersecurity is just one example.

There are few, if any aspects of human life that will not be impacted when fault-tolerant quantum computers – machines that no longer suffer from error and instability – become commonplace. With the rise of unprecedented computational power, however, there will be major new areas of ethical concern, including the acceleration of human DNA manipulation (Do we want to allow people to 'edit' their physical characteristics, for instance?); the creation of new materials for war; or an intrusive AI presence in most human activities.

In truth, far more areas will be impacted than we can imagine. Newton's oft-quoted description of the enormity of what lies ahead of us is strikingly appropriate in this context:

> I do not know what I may appear to the world; but to myself I seem to have been only like a boy playing on the sea-shore, and diverting myself in now and then finding a smoother pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me.

The COVID-19 pandemic has brought the world to a stark realization that despite the obvious benefits of globalization and the enormously beneficial ways in which technology has been adapted by societies in the past decades, there are still harrowing inequalities. One of the greatest challenges in quantum computing will be to determine how we can avoid a situation where an elite group of people or countries control quantum technologies.

It is true that once effective quantum computers are universally available, drugs and vaccines to protect us from some of the most horrible diseases such as cancer, Alzheimer's disease and COVID-19 will be developed more effectively and more quickly than is possible today. However, if issues around the tragedy experienced by society during the past year can serve as any sort of catalyst, we need to start thinking about how we can ensure that all of humanity can benefit from scientific advances.

Some of the more obvious questions are:

- How do we ensure that quantum computing's benefits will accrue to society as a whole and not just small portions?
- How do we ensure that we apply the principles of diversity throughout the entire quantum ecosystem that is now being developed?
- What happens when AI moves from a mere hypothesis used in trivial areas such as shopping recommendations to critical areas, including meaning-aware language processing that leads to the point where machines have unimaginably greater powers of communication than anything we have experienced?
- What about the extension of human longevity – a reality that quantum computing's ability to model molecular states could make more realizable?

These far-reaching implications only underscore the importance of timely ethical interventions. We were asleep at the wheel at the dawn of the internet era in the mid-1990s, but we can take lessons from the immediate past. Imagine if we had access to a magic time machine and could be transported back to 1995 – would we have let things develop in the way that they have?

Let's be brave and let's not wait until it's too late. Let's make sure that as a society we embrace this debate and we don't hold back.

There is in fact something even bigger at stake. Ask any scientist why they are excited by quantum computing, and they will say that quantum computers offer us a way to peer beyond the veil and understand the very nature of reality itself – truly, science for humanity.

We need to stay awake at the wheel this time and remain ever watchful, ready to address threats, mitigate possible harm and extend potential good universally so that we can deliver quantum technologies that bring the most benefit to the most people.

16 Feb 2021

21 Austria is getting a quantum internet

http://newsreadonline.com/austria-is-getting-a-quantum-internet/

Austria is getting a quantum internet. With the "Austrian Quantum Fiber Network" (AQUnet), an Austria-wide network of fiber optic cables is to be built that is suitable for the exchange of quantum information and precision measurements.

The Research Promotion Agency FFG is funding the project with 2.8 million euros, announced the Technical University (TU) Vienna. Initially, facilities in Vienna and Innsbruck are to be connected to the quantum Internet.

With the five-year project, the renowned quantum physics groups in Vienna and Innsbruck are to be "linked in a new way", explained the initiator of the project, Thorsten Schumm from the Atomic Institute of the Vienna University of Technology. The academic project partners include the Vienna University of Technology, the universities of Vienna and Innsbruck and the Federal Office for Metrology and Surveying (BEV).

There is also a group of first users such as the Austrian Academy of Sciences (ÖAW), the Austrian Institute of Technology (AIT) and the Institute of Science and Technology (IST) Austria. "We are assuming that further partners will join in the course of the project," said Schumm to the APA.

The project is coordinated by the ACOnet association as the operator of the "classic" high-performance data network that has been connecting domestic universities and research institutions with one another for decades. Depending on what is planned in the quantum Internet, fibers can be used that are already used for classic data transfer.

But there are also applications that can easily be disrupted. So-called "dark fibers" are required for these. These are light guides that are always laid as a reserve and are now to be used for the quantum Internet.

With the east-west connection within Austria, the foundation stone is to be laid "in order to then network further within Europe", explained Bernd Logar, Chairman of the ACOnet Association. There are similar initiatives in France, Germany and the Czech Republic, which represent possible starting points for the project.

Before that happens, there are still many questions to be answered. Because most of the previous experiments ran on fibers used purely for research between more or less neighboring laboratories. It must

now be clarified whether "a quantum Internet can be set up on an existing data backbone, what technical difficulties arise, what environmental influences there are, how far quantum information can be passed on without interference, etc.", emphasized Schumm.

The previous range of the most secure protocol for quantum communication is only a few tens of kilometers. This means that repeater stations have to be built in for the quantum Internet, but these are currently only being researched.

High precision measuring method

The possible applications are not limited to tap-proof quantum communication. The quantum network should also enable high-precision optical time and frequency measurement, Schumm refers to the expertise of his research group at the TU Vienna.

This would enable high-precision measuring methods; like how atomic clocks tick differently at different positions. This allows one to record tiny changes in the distance or height difference between the atomic clocks and thus "learn more about the behavior of the earth, including earthquake predictions," says Schumm.

In the past, you could call up the concert pitch A and thus a certified frequency of 440 Hertz over the telephone. An optical concert pitch A, which, however, oscillates at 194 terahertz, is supposed to be distributed over the quantum Internet in order to enable such highly precise measurements.

22 Myanmar's proposed cybersecurity Bill draws wide condemnation

by Eileen Yu

https://www.zdnet.com/article/myanmars-proposed-cybersecurity-bill-draws-wide-condemnation/

Myanmar's ruling military has drafted new cybersecurity laws that have been widely condemned as draconian, giving the government sweeping powers to access user data and block online sites. The legislation could also undermine the country's location as an offshore hub for data services, since it will not be in compliance with international laws.

News leaked days after the February 1 military coup that a draft copy of the Bill was sent to telcos and online service providers for their feedback, due back on Monday. According to various organisations that had seen the 36-page document, the proposed legislation would require online platforms operating in the country to retain all user data, including IP address, home address, and ID number, for three years and in a system assigned by the government.

In addition, Article 29 would enable the government to instruct a user account be intercepted, blocked, or removed when identified to incite hate or disrupt peace with "fake news", "disinformation, or comments that violated existing laws. Local authorities would also have access to the data when requested, without the need for a warrant.

The current military government, which has named itself the State Administration Council, pitched the proposed legislation as being necessary to combat cybercrime and various online activities deemed detrimental to the country.

Various organisations, though, have stepped up to condemn the rules as repressive, comprising vague

terms that would provide the government with powers to outlaw content and prosecute its author. It also marked a significant step back after years of economic and social progress in Myanmar, many have said.

In its statement, the Myanmar Centre for Responsible Business (MCRB) cautioned that such laws would not only impact civil society, but also risk driving away international investors and stymie local business growth, particularly in the ICT sector.

MCRB singled out the legislation's focus on data localisation of requiring data to be stored in sites designated by the government, which it said would leave local businesses vulnerable. This is especially true for banks and e-commerce companies that use significant volumes of data as they would not be able to tap the security and features offered by global cloud services, it said.

Financial services institutions, meanwhile, would not be able to mitigate security risks and ensure governance, and this would drive away foreign investors and harm local businesses already struggling to cope with the COVID-19 crisis, it added.

Myanmar's ability to create jobs and be a hub for offshore data-based services, such as call centres and shared service centres, would also be undermined as the proposed law would not be in compliance with international data protection rules, including the EU's General Data Protection Regulation (GDPR), said MCRB.

It noted that the Myanmar Computer Federation, Myanmar Computer Industry Association, and Myanmar Computer Professionals Association have already voiced their objections to the draft law.

Norwegian telecommunications group Telenor said in a statement Tuesday that the legislation should be debated in Parliament and consulted with industry stakeholders to ensure it was "fit for purpose" and in line with Myanmar's constitution.

Describing it as broad in scope, the company said the proposed laws would provide extensive powers that could "significantly impact many". The telco said its local operations, since 2013, were established on commitments from Myanmar's government that its regulatory updates and framework would be in line with international best practices. These included the establishment of an independent telecommunications regulator.

"We are concerned that the proposed bill does not progress relevant regulatory frameworks and law for a digital future, [neither does it] promote and safeguard digital safety and rights," Telenor said, adding that it was "not appropriate" to pass a bill with such broad powers to a temporary administration during a state of emergency.

It further called for the proposed Bill to adopt transparency and "legal certainty" with regards to the exercise of powers, and to exclude provisions that could be used to order interception of user accounts. It noted that laws governing personal data protection, electronic transactions, and cybersecurity should be kept separate to ensure governance.

In calling the proposed legislation "draconian", Human Rights Watch has urged for the laws to be withdrawn as they would "consolidate" the government's ability to conduct pervasive surveillance and cut access to essential services. The laws also neither specified how authorities would determine what constituted as misinformation nor provide any options for those whose content was blocked or removed to appeal, the organisation said.

Human Rights Watch's Asia legal advisor Linda Lakhdhir said: "The draft cybersecurity law would hand a military that just staged a coup and is notorious for jailing critics almost unlimited power to access user data, putting anyone who speaks out at risk."

Under the proposed rules, companies that fail to comply can face up to three years' imprisonment or fines of 10 million kyats ($7,009).

"The provisions of this cybersecurity law pose a clear threat to the right of Myanmar's citizens to reliable information and to the confidentiality of journalists' and bloggers' data," Daniel Bastard, Asia-Pacific head of Reporters Without Borders (RSF) said in a statement. "We urge digital actors operating in Myanmar, starting with Facebook, to refuse to comply with this shocking attempt to bring them to heel. This junta has absolutely no democratic legitimacy and it would be highly damaging for platforms to submit to its tyrannical impositions."

According to RSF, Facebook has almost 25 million users in the country or 45% of the local population. It added that access to the social media platform as well as others such as Twitter and Instagram was blocked soon after the February 1 coup.

UNI Global Union has also called for industry stakeholders to speak out against the law, singling out Japan's KDDI, Qatar's Ooredoo, and Telenor, as these three multinational corporations had strong presence in Myanmar.

Representing some 3 million employees in the ICT services sector, UNI Global Union's general secretary Christy Hoffman said: "This so-called cybersecurity bill only protects the government's grasp on power and it will be a powerful weapon against trade unionists, students, teachers, and the broad swath of civil society speaking out. The international community must stand up to reject this law... Telecommunications companies must also push back against this law or risk becoming a weapon of this military junta against democracy."

According to activist group Access Now, Myanmar's junta on Tuesday ordered another internet shutdown amidst increased military presence and use of force against demonstrators. It described the military's "weaponisation" of internet shutdowns to silence dissent as "unacceptable and a flagrant violation to human rights laws".

Access Now's Asia-Pacific policy director and senior international counsel, Jit Singh Chima, said: "Myanmar's draft cybersecurity bill is already instilling a fear of surveillance and being persecuted for what you say and do online. The gagging of telecom and ICT firms from being able to report on government orders concerning internet shutdowns, web censorship, or user surveillance is very concerning. Given the evolving situation and suppression of free media on the ground, the ability of telecom firms to provide information about the government directives they receive is key."

15 Feb 2021

23 How the defence industry benefits from rugged computing solutions

https://www.army-technology.com/sponsored/how-the-defence-industry-benefits-from-rugged-computing-solutions/

Industry 4.0 has seen exponential advancement in technological solutions across so many sectors, not only revolutionising the way that people work but expanding on what is possible. Digitalisation has shifted operations from pen-to-paper to computerised solutions, and the world of automation and analytics has propelled efficiency, safety and productivity.

Every sector presents its own challenges, and the defence industry is no different, so how can the industry utilise rugged computing solutions to keep their operations running as effectively as possible?

Army Technology spoke with rugged computing manufacturer Getac about its rugged devices and bespoke engineering solutions and exactly how they're moving the defence industry slowly but surely into industry 4.0

According to Getac's business development manager for defence, Rob Apple: "When it comes to digitalisation in the military, some advancements may not transfer across as quickly as the systems they have are often quite old. The military only just moved to Windows 10 in the last 18 months/two years. So one of the things that we are offer, because we have our own software engineers, is supporting legacy systems or legacy products."

He continues: "The difference with the military sector is that they take devices into a battlefield, which sounds obvious, but it's more than that. When you look at the other areas of a military operation, such as health care behind the front line, they still need the same capability as a normal hospital would.

"They have aircraft. They've got transportation. They've got fuel needs. They have people going around maintaining vehicles, maintaining equipment. The only difference in what we provide for the defence sector is that it can be in a dangerous or battleground environment."

Commanders can make more informed field decisions using Getac devices that are configurable with military data interfaces and encrypted communication, as well as access a web of networks, storage devices, servers and analysis software. Additionally, with so many factors involved in mission planning, anything that can be done by rote is welcome. Many Getac products for defence can be automated through the development of common components and software and shared across all platforms – such as aircraft and smart munitions.

Military operations rely on efficient and effective management to oversee transportation, tactical logistics and vehicle maintenance to ensure that vehicles are ready to be deployed and are communicating with their line of command. Getac MIL-461F certified devices allow ground forces to track and communicate with vehicles on the frontline. In cases of medical emergencies, Getac mobile solutions allow medical forces to access patient histories and forward casualty resuscitation information.

Getac's bespoke engineering offers complete system integration that meets military security requirements, offering customisations such as custom BIOS settings, asset tagging, and incorporation/installation of military connectors and legacy interfaces. Its computing solutions deliver high powered processing and reliability in adverse environments, as well as rugged casing to protect devices taken into the field.

However, no matter how rugged the device, in such hostile environments, equipment is exposed to numerous hazards that can result in devices breaking or failing. So should military operations have to worry about repeatedly needing to rebuy and replace their rugged devices?

According to Apple, though, this doesn't need to be the case: "We have bumper-to-bumper warranty that comes with all of our rugged devices. It covers everything – anything you can think of it will cover. We have examples with customers where devices have been crushed by tanks, flung across aircraft hangers after being left on helicopter rotors. "

"They then bring that to us," he continues, "and we handle it. It's a huge differentiator for Getac from our competitors – how comprehensive it is and that it covers everything aside from malicious damage.

"With some of our competitors, the display can only be repaired in a three-year warranty window, or the warranty will be pulled if there is repeated damage from the same fleet. With Getac you're getting superior products, incredible service and incomparable warranty coverage."

24 Light used to detect quantum information stored in 100,000 nuclear quantum bits

by University of Cambridge

https://phys.org/news/2021-02-quantum-nuclear-bits.html

Researchers have found a way to use light and a single electron to communicate with a cloud of quantum bits and sense their behavior, making it possible to detect a single quantum bit in a dense cloud.

The researchers, from the University of Cambridge, were able to inject a 'needle' of highly fragile quantum information in a 'haystack' of 100,000 nuclei. Using lasers to control an electron, the researchers could then use that electron to control the behavior of the haystack, making it easier to find the needle. They were able to detect the 'needle' with a precision of 1.9 parts per million: high enough to detect a single quantum bit in this large ensemble.

The technique makes it possible to send highly fragile quantum information optically to a nuclear system for storage, and to verify its imprint with minimal disturbance, an important step in the development of a quantum internet based on quantum light sources. The results are reported in the journal Nature Physics.

The first quantum computers – which will harness the strange behavior of subatomic particles to far outperform even the most powerful supercomputers – are on the horizon. However, leveraging their full potential will require a way to network them: a quantum internet. Channels of light that transmit quantum information are promising candidates for a quantum internet, and currently there is no better quantum light source than the semiconductor quantum dot: tiny crystals that are essentially artificial atoms.

However, one thing stands in the way of quantum dots and a quantum internet: the ability to store quantum information temporarily at staging posts along the network.

"The solution to this problem is to store the fragile quantum information by hiding it in the cloud of 100,000 atomic nuclei that each quantum dot contains, like a needle in a haystack," said Professor Mete Atatüre from Cambridge's Cavendish Laboratory, who led the research. "But if we try to communicate with these nuclei like we communicate with bits, they tend to 'flip' randomly, creating a noisy system."

The cloud of quantum bits contained in a quantum dot don't normally act in a collective state, making it a challenge to get information in or out of them. However, Atatüre and his colleagues showed in 2019 that when cooled to ultra-low temperatures also using light, these nuclei can be made to do 'quantum dances' in unison, significantly reducing the amount of noise in the system.

Now, they have shown another fundamental step towards storing and retrieving quantum information in the nuclei. By controlling the collective state of the 100,000 nuclei, they were able to detect the existence of the quantum information as a 'flipped quantum bit' at an ultra-high precision of 1.9 parts per million: enough to see a single bit flip in the cloud of nuclei.

"Technically this is extremely demanding," said Atatüre, who is also a Fellow of St John's College. "We don't have a way of 'talking' to the cloud and the cloud doesn't have a way of talking to us. But what we can talk to is an electron: we can communicate with it sort of like a dog that herds sheep."

Using the light from a laser, the researchers are able to communicate with an electron, which then communicates with the spins, or inherent angular momentum, of the nuclei.

By talking to the electron, the chaotic ensemble of spins starts to cool down and rally around the shepherding electron; out of this more ordered state, the electron can create spin waves in the nuclei.

"If we imagine our cloud of spins as a herd of 100,000 sheep moving randomly, one sheep suddenly changing direction is hard to see," said Atatüre. "But if the entire herd is moving as a well-defined wave, then a single sheep changing direction becomes highly noticeable."

In other words, injecting a spin wave made of a single nuclear spin flip into the ensemble makes it easier to detect a single nuclear spin flip among 100,000 nuclear spins.

Using this technique, the researchers are able to send information to the quantum bit and 'listen in' on what the spins are saying with minimal disturbance, down to the fundamental limit set by quantum mechanics.

"Having harnessed this control and sensing capability over this large ensemble of nuclei, our next step will be to demonstrate the storage and retrieval of an arbitrary quantum bit from the nuclear spin register," said co-first author Daniel Jackson, a Ph.D. student at the Cavendish Laboratory.

"This step will complete a quantum memory connected to light – a major building block on the road to realizing the quantum internet," said co-first author Dorian Gangloff, a Research Fellow at St John's College.

Besides its potential usage for a future quantum internet, the technique could also be useful in the development of solid-state quantum computing.

25 New AI 'Ramanujan Machine' uncovers hidden patterns in numbers

by Stephanie Pappas

https://www.livescience.com/ramanujan-machine-created.html

A new artificially intelligent "mathematician" known as the Ramanujan Machine can potentially reveal hidden relationships between numbers.

The "machine" consists of algorithms that seek out conjectures, or mathematical conclusions that are likely true but have not been proved. Conjectures are the starting points of mathematical theorems, which are conclusions that have been proved by a series of equations.

The set of algorithms is named after Indian mathematician Srinivasa Ramanujan. Born in 1887 to a store clerk and a homemaker, Ramanujan was a child prodigy who came up with many mathematical conjectures, proofs and solutions to equations that had never before been solved. In 1918, two years before his early death from disease, he was elected as a Fellow of The Royal Society London, becoming only the second Indian man to be inducted after marine engineer Ardaseer Cursetjee in 1841.

Ramanujan had an innate feel for numbers and an eye for patterns that eluded other people, said physicist Yaron Hadad, vice president of AI and data science at the medical device company Medtronic and one of the developers of the new Ramanujan Machine. The new AI mathematician is designed to pull out promising mathematical patterns from large sets of potential equations, Hadad told Live Science, making Ramanujan a fitting namesake.

Math by machine

Machine learning, in which an algorithm detects patterns in large amounts of data with minimal direction from programmers, has been put to use in a variety of pattern-finding applications, from image

recognition to drug discovery. Hadad and his colleagues at the Technion-Israel Institute of Technology in Haifa wanted to see if they could use machine learning for something more fundamental.

"We wanted to see if we could apply machine learning to something that is very, very basic, so we thought numbers and number theory are very, very basic," Hadad told Live Science.

Already, some researchers have used machine learning to turn conjectures into theorems – a process called **automated theorem proving**. The goal of the Ramanujan Machine, instead, is to identify promising conjectures in the first place. This has previously been the domain of human mathematicians, who have come up with famous proposals such as Fermat's Last Theorem[1], which claims that there are no three positive integers that can solve the equation $a^n + b^n = c^n$ when $n > 2$.

To direct the Ramanujan Machine, the researchers focused on fundamental constants, which are numbers that are fixed and fundamentally true across equations. The most famous constant might be the ratio of a circle's circumference to its diameter, better known as π. Regardless of the size of the circle, that ratio is always 3.14159265 . . . and on and on.

The algorithms essentially scan large numbers of potential equations in search of patterns that might indicate the existence of formulas to express such a constant. The programs first scan a limited number of digits, perhaps five or 10, and then record any matches and expand upon those to see if the patterns repeat further.

When a promising pattern appears, the conjecture is then available for an attempt at a proof. More than 100 intriguing conjectures have been generated so far, Hadad said, and several dozen have been proved.

A community effort

The researchers reported their results Feb. 3 in the journal Nature. They have also set up a website, RamanujanMachine.com, to share the conjectures the algorithms generate and to collect attempted proofs from anyone who'd like to take a stab at discovering a new theorem. Users can also download the code to run their own searches for conjectures, or let the machine use their spare processing space on their own computers to look on its own. Part of the goal, Hadad said, is to get lay people more involved in the world of mathematics.

The researchers also hope that the Ramanujan Machine will help change how math is done. It's hard to say how advances in number theory will translate to real-world applications, Hadad said, but so far, the algorithm has helped uncover a better measure of irrationality for Catalan's constant, a number denoted by G that has at least 600,000 digits but may or may not be an irrational number. (An irrational number cannot be written as a fraction; a rational number can.) The algorithm hasn't yet answered the question of whether Catalan's constant is or isn't rational, but it's moved a step closer to that goal, Hadad said.

"We are still in the very early stages of this project, where the full potential is only starting to unfold," he told Live Science in an email. "I believe that generalizing this concept to other areas of mathematics and physics (or even other fields of science) will enable researchers to get leads to new research from computers. So human scientists will be able to choose better goals to work on from a wider selection offered by computers, and thus improve their productivity and potential impact on human knowledge and future generations."

14 Feb 2021

[1]That famous conjecture was scribbled in the margins of a book by mathematician Pierre de Fermat in 1637 but wasn't proven until 1994.

26 how new technology could power quantum computing?

by Vivek Kumar

https://www.analyticsinsight.net/quantum-leap-how-new-technology-could-power-quantum-computing/

Quantum computing promises huge possibilities for the development of individuals, societies and corporations. From academic practices to big business development, quantum computing is transforming everything. As the technology for building quantum computers is starting to gain momentum, superconductors are becoming more valuable embraced by tech giants such as IBM and Intel. A set of physical properties observed in certain materials, superconductors conduct electricity without resistance when it becomes colder than a critical temperature. They are widely used in medical imaging, electronic devices, magnetic shielding, quantum PCs, etc.

As superconductors provide a macroscopic glimpse into quantum phenomena, they are often expensive to manufacture and prone to err from environmental noise. However, in an effort to change that, researchers from Karl Berggren's group in the Department of Electrical Engineering and Computer Science are developing a superconducting nanowire. It could enable more efficient superconducting electronics. According to Berggren, the nanowire's potential benefits derive from its simplicity.

According to the paper, most metals lose resistance and become superconducting at extremely low temperatures, just a few degrees above absolute zero. They are used to sense magnetic fields, especially in highly-sensitive situations like monitoring brain activity. They also have applications in both quantum and classical computing. Underlying such superconductors is a device invented in the 1960s called the Josephson junction that is fundamentally quite a delicate object. However, it is costly and complex to manufacturing, especially for thin insulators. Josephson junction-based superconductors also may not play well with others, Berggren noted. This lack of ability to control larger-scale objects is a real drawback when trying to interact with the outside world. This is where Berggren's superconducting nanowire plays a crucial role.

In 1956, an electrical engineer at MIT, Dudley Buck published a description of a superconducting computer switch called the cryotron, which was little more than two superconducting wires. One was straight and the other was coiled around it. The cryotron performs as a switch, and when current flows through the coiled wire, its magnetic field lessens the current flowing through the straight wire. Now, researchers from Berggren's group are revitalizing Buck's ideas about superconducting computer switches.

Their superconducting nanowire device, dubbed as nano-cryotron, uses heat to trigger a switch, rather than a magnetic field. Current in this device runs through a superconducting, supercooled wire called the channel. Researchers have already demonstrated proof-of-concept for the nano-cryotron's use as an electronic component. According to Berggren, the superconducting nanowire could one day complement – or perhaps compete with – Josephson junction-based superconducting devices.

Today, many big companies are racing to quantum supremacy that has long been seen as a milestone for quantum computers. In October 2019, Google announced that it had achieved quantum supremacy with a machine that performed a particular calculation. Last year, multinational conglomerate Honeywell announced that it had achieved a breakthrough in quantum computing that expedites the capability of quantum computers.

More broadly, quantum computing is expected to perform complex computations faster and more efficiently than the most powerful supercomputers available today. This significant acceleration could

expand the scope of computing, revolutionizing the industry, economy and society.

27 Cybersecurity experts say U.S. needs to strike back after SolarWinds hack

by Will Croxton

https://www.cbsnews.com/news/solarwinds-60-minutes-2021-02-14/

In March of last year, thousands of companies and U.S. government agencies were sent a routine software update. This happened regularly with SolarWinds Orion software. There was no reason to suspect anything was wrong with the update.

What they couldn't see at the time was a malicious piece of code buried deep within the update, a Trojan horse planted by Russian cyber soldiers looking for a backdoor to important American computer networks.

Nine months after that compromised software update, cybersecurity firm FireEye sounded the alarm. They had been hacked. Their crown jewels, what the company calls "Red Team tools," had been stolen. FireEye suspected that anyone who had downloaded and installed the SolarWinds Orion update had been hacked too.

While the full extent of the SolarWinds exploit is still not known, the information gleaned so far is concerning. The U.S. Treasury Department, Department of Justice, State Department, Energy Department, and the agency that protects and transports the U.S. nuclear arsenal, didn't see the Russians rummaging through their computer networks for nine months. Businesses, including software titan Microsoft, have also found their systems compromised by the update. SolarWinds says its products are used by 300,000 customers around the globe, and that 18,000 customers downloaded its compromised software update. More companies are expected to learn they were victims of the hack.

"This was an act of cyber terrorism," said Jon Miller, CEO of Boldend, which designs and sells cyber weapons to U.S. intelligence agencies. "The goal behind this was fear."

60 Minutes spoke to three cybersecurity experts who say they believe the U.S. government's current strategy for cyber warfare is inadequate and does not effectively deter its adversaries in cyberspace. They warn that if the U.S. government doesn't change course, the hacks will keep coming.

clear lines and effective consequences

Jon Miller, a former "ethical hacker," said the U.S. is allowing this malign activity to happen. "We're letting them do this," he said. "And there's no repercussions to them whatsoever."

Miller said indictments against international hackers often don't lead to arrests. "The government will track down the individuals that were responsible in this breach. They won't get arrested though," he explained. "It just means that they can never travel to the U.S. And they get to continue hacking us day, after day, after day with no consequence in sight."

He suggested that the U.S. needs to define clear red lines for our adversaries and a commitment to attack if they are crossed. "We haven't drawn a line and said, 'This is enough. You have to stop attacking us, or we are willing to escalate it,'" he said. "We're not willing to attack. And that's what we're missing now. There's no capability that the United States has that scares them enough to not attack us."

a collaboration of defenders

Chris Inglis, a former deputy director of the NSA, said the separation between government and private enterprise, while bound by law and in line with American values, makes coordination on cyber defense difficult. Without a united line of defense, that separation can be exploited by an aggressor.

"It turns out that a division of effort is actually an agreement to not collaborate," he said. "One party's attempting to defend their patch and another party's defending their patch. Both sides are ignorant. And the aggressor can pick you off one at a time."

Inglis now works on the Cyberspace Solarium Commission, created by Congress to advise the legislative branch on cyber defense matters. He suggested greater collaboration between government and private business to identify and address cyber threats. "Unless there's some collaboration of the defenders," he explained, "No one person is going to have the god's eye view of what's happening in that network."

a call to fight back

James Lewis, a director at the Center for Strategic and International Studies, said fear of escalation has held the U.S. back from punishing Russia, and other nation states, when they step out of line. "Escalation's a reasonable concern. But it shouldn't be enough to say, 'Oh, we shouldn't do anything because the Russians might be mad,'" he said. "The goal is to make them mad. The goal is to make them afraid. How do you punish the Russians without triggering a major conflict?"

He suggested the U.S. experiment with tactics to find creative ways of inflicting revenge on Russia. "Could you interfere with their media? Could you start putting stories in the Russian media?" he offered. "The one that bothers them the most is corruption because it creates the popular discontent in their own populations that they don't want."

He said interfering with money allegedly stashed away in other financial systems by powerful Russians in government and business could be another deterrent. "We could interfere a little bit with their financial activities," the Center for Strategic and International Studies' Lewis suggested. "They have money squirreled all around the world."

James Lewis retains hope that the Biden administration will be more willing to explore an offensive strategy with the Russians, and other nations like China, who attack the U.S. in cyberspace. "[Biden] could rethink how we use the exquisite capabilities that NSA and Cyber Command have to inflict pain on Russia and the others," he said. "It's risky. But if we don't take risk, we're not gonna be able to work our way out of this."

12 Feb 2021

28 Microsoft's Big Win in Quantum Computing Was an 'Error' After All

by tom simonite

https://www.wired.com/story/microsoft-win-quantum-computing-error/

Dutch physicist and Microsoft employee Leo Kouwenhoven published headline-grabbing new evidence that he had observed an elusive particle called a Majorana fermion.

Microsoft hoped to harness Majorana particles to build a quantum computer, which promises unprecedented power by tapping quirky physics. Rivals IBM and Google had already built impressive prototypes using more established technology. Kouwenhoven's discovery buoyed Microsoft's chance to catch up. The company's director of quantum computing business development, Julie Love, told the BBC that Microsoft would have a commercial quantum computer "within five years."

Three years later, Microsoft's 2018 physics fillip has fizzled. Late last month, Kouwenhoven and his 21 coauthors released a new paper including more data from their experiments. It concludes that they did not find the prized particle after all. An attached note from the authors said the original paper, in the prestigious journal Nature, would be retracted, citing "technical errors."

Two physicists in the field say extra data Kouwenhoven's group provided them after they questioned the 2018 results shows the team had originally excluded data points that undermined its news-making claims. "I don't know for sure what was in their heads," says Sergey Frolov, a professor at the University of Pittsburgh, "but they skipped some data that contradicts directly what was in the paper. From the fuller data, there's no doubt that there's no Majorana."

The 2018 paper claimed to show firmer evidence for Majorana particles than a 2012 study with more ambiguous results that nevertheless won fame for Kouwenhoven and his lab at Delft Technical University. That project was partly funded by Microsoft, and the company hired Kouwenhoven to work on Majoranas in 2016.

The 2018 paper reported seeing telltale signatures of the Majorana particles, termed "zero-bias peaks," in electric current passing through a tiny, supercold wire of semiconductor. One chart in the paper showed dots tracing a plateau at exactly the electrical conductance value that theory predicted.

Frolov says he saw multiple problems in the unpublished data, including data points that strayed from the line but were omitted from the published paper. If included, those data points suggested Majorana particles could not be present. Observations flagged by Frolov are visible in the charts in the new paper released last month, but the text does not explain why they were previously excluded. It acknowledges that trying to experimentally validate specific theoretical predictions "has the potential to lead to confirmation bias and effectively yield false-positive evidence."

Microsoft provided a statement attributed to Kouwenhoven saying he could not comment, because the new paper that reinterprets his group's results is undergoing peer review. "We are confident that scaled quantum computing will help solve some of humanity's greatest challenges, and we remain committed to our investments in quantum computing," he said. Nature added an "editorial expression of concern" to the 2018 paper in April last year, and a spokesperson said this week that the journal is "working with the authors to resolve the matter." A spokesperson for Delft Technical University said an investigation by its research integrity committee, started in May 2020, is not complete. A person familiar with the process says the final report will likely find that researchers at Delft made mistakes but did not intend to mislead.

Whatever happened, the Majorana drama is a setback for Microsoft's ambitions to compete in quantum computing. Leading computing companies say the technology will define the future by enabling new breakthroughs in science and engineering.

Quantum computers are built from devices called qubits that encode 1s and 0s of data but can also use a quantum state called a superposition to perform math tricks not possible for the bits in a conventional computer. The main challenge to commercializing that idea is that quantum states are delicate and easily

quashed by thermal or electromagnetic noise, making qubits error-prone.

Google, IBM, and Intel have all shown off prototype quantum processors with around 50 qubits, and companies including Goldman Sachs and Merck are testing the technology. But thousands or millions of qubits are likely required for useful work. Much of a quantum computer's power would probably have to be dedicated to correcting its own glitches.

Microsoft has taken a different approach, claiming qubits based on Majorana particles will be more scalable, allowing it to leap ahead. But after more than a decade of work, it does not have a single qubit.

Majorana fermions are named after Italian physicist Ettore Majorana, who hypothesized in 1937 that particles should exist with the odd property of being their own antiparticles. Not long after, he boarded a ship and was never seen again. Physicists wouldn't report a good glimpse of one of his eponymous particles until the next millennium, in Kouwenhoven's lab.

Microsoft got interested in Majoranas after company researchers in 2004 approached tech strategy chief Craig Mundie and said they had a way to solve one problem holding back quantum computers – qubits' flakiness.

The researchers seized on theoretical physics papers suggesting a way to build qubits that would make them more dependable. These so-called topological qubits would be built around unusual particles, of which Majorana particles are one example, that can pop into existence in clumps of electrons inside certain materials at very low temperatures.

Microsoft created a new team of physicists and mathematicians to flesh out the theory and practice of topological quantum computing, centered on an outpost in Santa Barbara, California, christened Station Q. They collaborated with and funded leading experimental physicists hunting for the particles needed to build this new form of qubit.

Kouwenhoven, in Delft, was one of the physicists who got Microsoft's backing. His 2012 paper reporting "signatures" of Majorana particles inside nanowires started chatter about a future Nobel prize for proving the elusive particles' existence. In 2016, Microsoft stepped up its investment – and the hype.

Kouwenhoven and another leading physicist, Charles Marcus, at the University of Copenhagen were hired as corporate Majorana hunters. The plan was to first detect the particles and then invent more complex devices that could control them and function as qubits. Todd Holmdahl, who previously led hardware for Microsoft's lucrative Xbox games console, took over as leader of the topological quantum computing project. Early in 2018, he told Barron's he would have a topological qubit by the end of the year. The now-disputed paper appeared a month later.

While Microsoft sought Majoranas, competitors working on established qubit technologies reported steady progress. In 2019, Google announced it had reached a milestone called quantum supremacy, showing that a chip with 53 qubits could perform a statistical calculation in minutes that would take a supercomputer millennia. Soon after, Microsoft appeared to hedge its quantum bet, announcing it would offer access to quantum hardware from other companies via its cloud service Azure. The Wall Street Journal reported that Holmdahl left the project that year after missing an internal deadline.

Microsoft has been quieter about its expected pace of progress on quantum hardware since Holmdahl's departure. Competitors in quantum computing continue to tout hardware advances and urge software developers to access prototypes over the internet, but none appear close to creating a quantum computer ready for prime time.

Frolov, the University of Pittsburgh researcher, says the questions around Kouwenhoven's 2018 paper

leave the small field of physics dedicated to detecting Majoranas "wounded," facing a potentially unpleasant comedown after a period of high expectations. "We have good science to do with reasonable expectations, not magical expectations," he says. Frolov says the group should release the full raw data from its experiments for outside scrutiny.

Frolov worked through the extra data with Vincent Mourik from Australia's University of New South Wales, who says he shares Frolov's concerns. Both previously worked with Kouwenhoven at Delft, before he was hired by Microsoft, including on the 2012 paper on Majorana particles.

Sankar Das Sarma, a theoretical physicist at the University of Maryland who has collaborated with Microsoft researchers, believes the technology will eventually work, but it could take a while. He was a coauthor on both the disputed 2018 paper and the new version posted last month.

Das Sarma says new theories developed over the past few years show that the methodology used in 2018 could not conclusively establish the presence of Majorana particles anyway. Purer materials, more complex experiments, and a lot more scientific progress are all needed, he says.

How far off that puts a Microsoft qubit is unclear. Das Sarma says Majorana-based quantum computing may be at a stage comparable to 1926, when the first patent for a transistor was filed. It took until 1947 for researchers to create the first working transistor; the miniaturizable silicon versions that enabled the computing industry were not developed until the late 1950s. "I see no reason why a Majorana fermion cannot exist or that once it exists you cannot control it," he says. "But it may be 30 years away."

29 Quantum Computers: IBM Outlines its Development Roadmap

by Maurizio Di Paolo Emilio

https://www.eetimes.eu/quantum-computers-ibm-outlines-its-development-roadmap/

Quantum computing is at a pivotal point. The decisive quantum leap could be coming. IBM has outlined its quantum computing development roadmap that will begin with the release of the **Qiskit Runtime open-source software in 2021**.

In an interview with EE Times Europe, Bob Sutor, vice president of Quantum Ecosystem Development at IBM, pointed out that currently no one is yet using quantum computers in production. The challenge will be to make this new environment more and more accessible and allow companies and developers to experiment with the release of applications. Besides software aspects, the increasingly efficient hardware with a decidedly high qubit count will pave the way for commercial applications. In any case, in the near future, quantum computers will not replace classical computers. They will work together.

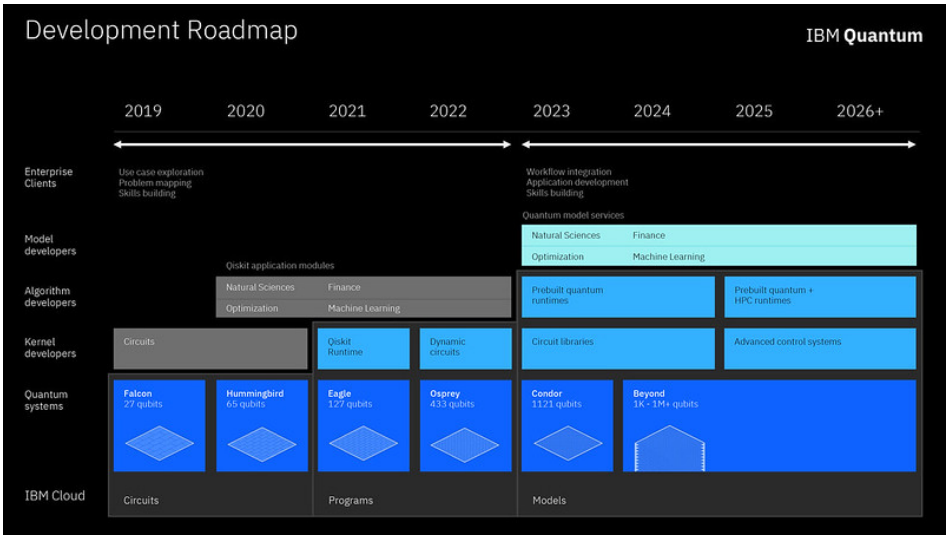
In September 2020, IBM highlighted how they took the bold step of releasing a hardware roadmap that shows a clear path to over 1000 qubits and identified challenges along the way. This time around, there will be the open-source community and the ability to mobilize developers around the world, plus cloud-native deployment to break down critical challenges and democratize access to this new technology as quickly as possible.

IBM and open-source developers will work to optimize the foundation of the stack. Simultaneously, other kernel developers are deploying high-performance quantum circuits with increasingly sophisticated performance mechanisms, paving the way to develop models for chemistry, physics, biology, machine learning, optimization, or even finance.

"Our new development roadmap provides new opportunities for collaboration. We are increasing the variety of circuits and the ability of our systems to run more circuits faster. The roadmap is pointing out beyond 2023, when we will get above 1000 qubits. Then, we can seriously address things like error correction, and look at Quantum Advantage, which is the point where quantum systems together with classical systems can do much better than just classical systems by themselves," said Sutor.

He added, "the ability to reliably manage the operation and control of different quantum systems was not possible just a few years ago. Today, we can increase the number of qubits, thanks to extraordinary efforts in science and engineering."

The implementation of the roadmap will be done in stages. It will include the implementation of high-performance quantum software and hardware. The development of new quantum algorithms will build on the foundation of innovative quantum circuits, thus the development of programs or applications. On top of the algorithms, complex programs and models will be used in various industry fields.



Hardware for quantum computing

It will take another few years for us to see commercial applications in production. In the meantime, many leading companies are developing ambitious quantum computing programs. A number of startups are investing in quantum computing especially in Error Quantum Correction and Cryptography.

In 2001, IBM developed the first 7-qubit quantum processor. In 2016, IBM released the first quantum system openly available on the cloud. IBM now has approximately 20 computers in the cloud available to users for free.

IBM plans to reach 127 qubit quantum computers by the end of 2021, 433 qubits before the end of next year, and more than 1000 qubits by 2023.

The company's newly released processor, **IBM Quantum Hummingbird**, is 65 qubits. Next year, it will be **IBM Quantum Eagle**, at 127 qubits, while in 2023 it expects to release **IBM Quantum Condor**, a processor at 1121 qubits. They expect eventual quantum computing applications in the field of neural networks moving to the realization of economic models, from the study of personalized drugs to simulations of complex chemical reactions up to many other possibilities such as the optimization of mathematical problems and some parts of artificial intelligence.

The IBM Quantum Eagle chip will feature several upgrades to reduce qubit errors and will continue to lay the groundwork for scaling the number of qubits that work together as logical qubits. IBM pointed out that, with the Eagle processor, real-time classical compute capabilities will be introduced for execution of a broader family of quantum circuits and codes.

Qubits

In quantum computers, the bits, i.e., the basic information unit of classical computers, are replaced by the so-called "qubits", quantum bits, which are able to cope with enormously complex problems thanks to a greater possibility of encoding information. Problems that are largely out of reach for normal computers. Like classical computers that include logic gates and circuits, a quantum computer uses quantum circuits composing elementary quantum logic gates.

Quantum computers use three concepts. The first is the "quantum superposition", the idea behind Schrödinger's living and dead cat. Unlike the classic bits, that can only have two states – one or zero -, the "qubits" states can be a combination of both. The second is "entanglement". It correlates quantum particles together through time and space. The third is interference, where we can design algorithms so that the "right answers" are more likely to appear than the wrong.

Open source for quantum computing

IBM has specified that quantum computers will be particularly useful in certain areas: Life sciences, chemistry, and artificial intelligence. In these areas, the open-source software Qiskit will be able to accelerate certain computational tasks. This year, IBM will release the Qiskit Runtime – an execution environment that increases the capacity to run more circuits at a much faster rate than ever before. This increases the capacity of a quantum computer to do more work.

And just to make the most of Qiskit's capabilities, IBM is expanding the pool of developers involved in the project. "We've trained thousands people to use Qiskit, and the software has been downloaded by developers more than half a million times," said Sutor.

He added, "With this roadmap, we are talking about how to improve our systems in three different ways. The first is quality. How well will circuits do what they are supposed to do? This is the Quantum Volume discussion. It includes things like error mitigation and reduction of noise. The second thing is capacity. How fast are your machines? We aim to run circuits 100 times faster by the end of the year. The increased capacity gives me more time to run more circuits. And the third type is variety, that is, getting the benefits of quantum with some of the most interesting features of classical coding."

Qiskit provides a set of code tools for quantum circuit-level programs, offering execution and management on remote access back ends. IBM is making the functions very simple even for those who are not experts in quantum theory or quantum mechanics, which is the basis of a quantum computer. The goal is to offer a wider variety of circuits, allowing users to tackle problems unsolvable with classical computers. Software tools such as OpenQASM 3 will soon offer quantum kernel developers the ability to run dynamic circuits – those that incorporate both classical and quantum instructions that must be executed within the coherence time of qubits – by 2022. Sutor pointed out that in 2023 there will be new advanced control systems to manipulate large amounts of qubits to provide the full benefit of quantum computing.

30 The Interplay between Quantum Theory And Artificial Intelligence

by ambika choudhury

https://analyticsindiamag.com/the-interplay-between-quantum-theory-and-artificial-intelligence/

Machine Learning Developers Summit (MLDS 2021) is one of the biggest gatherings of machine learning developers in India. With more than 1,500 machine learning developers, 60 speakers from around 200 organisations, the conference corrals India's leading Machine Learning innovators and practitioners to share their ideas about machine learning tools, advanced development and more.

Anish Agarwal, Director, Data & Analytics, India at NatWest Group, talked about "The Interplay between Quantum Theory And Artificial Intelligence" at MLDS 2021.

The session started with an introduction to emerging technologies like artificial intelligence, a brief on quantum computing, different forms of quantum technology used for various military as well as civilian applications, how it is different from the classical computers as well as how quantum computing plays a vital role in the advancement of artificial intelligence.

In the field of quantum computing, Agarwal discussed the technique of quantum artificial intelligence, how it can be used for computation of machine learning algorithms and what makes this technology unique.

Quantum AI can help in achieving results that are impossible with classical computers. He said, as per reports, 25% of fortune global 500 companies will have a competitive edge from quantum computing by the year 2023. Tech giants like Google, Microsoft are doubling down on quantum computing.

He then explained the possibilities of applying quantum computing in AI:

- **Quantum Algorithms for Learning:** Specifically for machine learning, quantum algorithms for learning can provide possible speedups and other improvements in a deep learning training process. The contribution of quantum computing to classical machine learning can be achieved by presenting the optimal solution at the base of artificial neural networks.
- **Quantum Search:** Quantum search algorithm can be described as a database search algorithm.
- **Quantum Algorithms for Decision Problems:** Quantum algorithms based on Hamiltonian time evaluation can solve problems faster than classical algorithms.

He said, "Quantum machine learning (QML) is not one settled homogeneous field. This is because machine learning itself is quite diverse in nature." He added, "Quantum Machine Learning is simply the field exploring the connections between quantum computing and quantum physics on one hand and machine learning and related fields on the other hand."

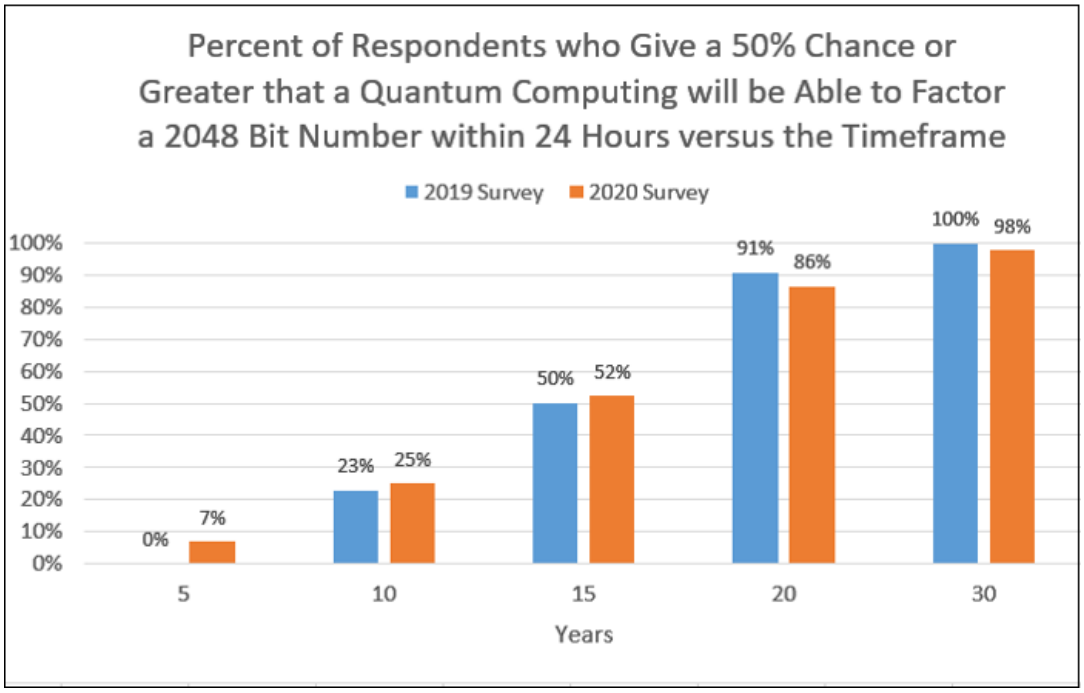
Agarwal then deliberated on Quantum Game Theory and compared it with classical game theory. He said quantum game theory can be used to overcome critical problems in quantum communications.

31 Quantum Threat Timeline Report 2020

https://quantumcomputingreport.com/quantum-threat-timeline-report-2020/

A fascinating study has been published by the Global Risk Institute. It was created by Dr. Michele Mosca and Dr. Marco Piani of evolutionQ and is an update to a study published a year ago that surveyed noted academics and researchers on when they predict a quantum computer would be available that could factor a 2048 bit number and break the RSA encryption code. The 2019 study asked 22 researchers to estimate the likelihood that such a powerful quantum computer would appear within timeframes of 5, 10, 15, 20, and 30 years. The 2020 study expanded the experts survey to 44 respondents from 14 different countries and included additional questions on the expected level of funding for quantum research as well as the impact that Covid-19 has had on quantum research. We will summarize a few of the conclusions in this rest of this article and provide a link to the full report below.

To start, the survey asked the experts their assessment of the likelihood a quantum computer could factor a 2048 bit number within a 24 hour time period versus the time frame. The graph below shows the%age of experts who assessed the likelihood to be 50% or greater in both the 2019 study and the 2020 study. The results are similar with the 2020 survey being slightly higher in the 10-15 year periods. But that is probably due to the fact that the industry has just completed one more year of development.



Other questions posted included getting the experts opinions on ranking different implementation technologies by their potential to realize a digital quantum computer with 100 qubits within the next 15 years. The ranking for the technologies based upon the number of times the technology was called out as the first or second choice is shown below. The superconducting and trapped ion technologies were ranked far ahead of the others.

(i) Superconducting

(ii) Trapped Ions

(iii) Quantum Optics

(iv) Spin Systems in Silicon

(v) Spin Systems Not in Silicon

(vi) Cold Atoms

(vii) Other

(viii) Topological

Another interesting survey topic was their expectation on whether the level of funding from government and industry would increase, stay the same, or decrease within the next two years. Based upon the responses below, there does not seem to be any likelihood of a quantum winter in the next couple of years.

Significant Increase	23%
Increase	42%
Same	28%
Decrease	5%
Not Specified	2%

The full report is 52 pages and provides a ton of data analyzed in many different ways. In addition, it contains many qualitative comments from the respondents that we think you would find interesting. Readers interested in understanding the views of these quantum thought leaders can download the full 2020 report available on the Global Risk Institute website.

32 Microsoft launches new hybrid cloud solution in India

by Ishan Patra

https://www.thehindu.com/sci-tech/technology/microsoft-launches-new-hybrid-cloud-solution-in-india/article33819944.ece

Microsoft on Thursday launched a new hybrid cloud solution in India for organisations to build and run cloud-native applications with seamless access to on-premise cloud services with existing tool, processes, and skillsets.

Azure Stack hyperconverged infrastructure (HCI), the new addition to the Azure Stack portfolio is compatible with both Windows and Linux virtual machines, and will be available from 20 partners offering Microsoft-validated hardware systems.

“The role of hybrid cloud has transformed from being integrator of datacentres with the public cloud to enabler of day-to-day business functions,” Microsoft India COO Rajiv Sodhi, said in a statement. “Consistent hybrid tools and experiences have never been more important and Azure Stack HCI brings together the familiarity and flexibility of on-premises virtualisation with powerful new hybrid capabilities.”

Azure Stack HCI combines infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) services in a software stack that spans on-premises datacentres and Microsoft’s Azure cloud, providing the latest and up to date security, performance, and feature updates.

The software giant’s new hybrid cloud solution can be scaled according to the workload of enterprises and provides access to familiar tools from the company as well as popular third-party tools. Organisations can opt for Microsoft’s pay-as-you-go subscription model for flexibility and lower total cost of ownership, the company noted.

"With our cloud-native approach, we aim to help customers realise higher value HCI through quick deployment and integration that leverages familiar management and tools with flexible Azure subscription pricing," Sodhi said. "This will enable organisations to be adaptive, agile, efficient, and responsive across locations, optimising operations and IT cost efficiency in an increasingly remote work environment today."

33 Applying Quantum Computing to a Particle Process

by Glenn Roberts Jr.

https://newscenter.lbl.gov/2021/02/12/applying-quantum-computing-to-a-particle-process/

A team of researchers at Lawrence Berkeley National Laboratory (Berkeley Lab) used a quantum computer to successfully simulate an aspect of particle collisions that is typically neglected in high-energy physics experiments, such as those that occur at CERN's Large Hadron Collider.

The quantum algorithm they developed accounts for the complexity of parton showers, which are complicated bursts of particles produced in the collisions that involve particle production and decay processes.

Classical algorithms typically used to model parton showers, such as the popular Markov Chain Monte Carlo algorithms, overlook several quantum-based effects, the researchers note in a study published online Feb. 10 in the journal Physical Review Letters that details their quantum algorithm.

"We've essentially shown that you can put a parton shower on a quantum computer with efficient resources," said Christian Bauer, who is Theory Group leader and serves as principal investigator for quantum computing efforts in Berkeley Lab's Physics Division, "and we've shown there are certain quantum effects that are difficult to describe on a classical computer that you could describe on a quantum computer." Bauer led the recent study.

Their approach meshes quantum and classical computing: It uses the quantum solution only for the part of the particle collisions that cannot be addressed with classical computing, and uses classical computing to address all of the other aspects of the particle collisions.

Researchers constructed a so-called "toy model," a simplified theory that can be run on an actual quantum computer while still containing enough complexity that prevents it from being simulated using classical methods.

"What a quantum algorithm does is compute all possible outcomes at the same time, then picks one," Bauer said. "As the data gets more and more precise, our theoretical predictions need to get more and more precise. And at some point these quantum effects become big enough that they actually matter," and need to be accounted for.

In constructing their quantum algorithm, researchers factored in the different particle processes and outcomes that can occur in a parton shower, accounting for particle state, particle emission history, whether emissions occurred, and the number of particles produced in the shower, including separate counts for bosons and for two types of fermions.

The quantum computer "computed these histories at the same time, and summed up all of the possible histories at each intermediate stage," Bauer noted.

The research team used the IBM Q Johannesburg chip, a quantum computer with 20 qubits. Each qubit, or quantum bit, is capable of representing a zero, one, and a state of so-called superposition in which it

represents both a zero and a one simultaneously. This superposition is what makes qubits uniquely powerful compared to standard computing bits, which can represent a zero or one.

Researchers constructed a four-step quantum computer circuit using five qubits, and the algorithm requires 48 operations. Researchers noted that noise in the quantum computer is likely to blame for differences in results with the quantum simulator.

While the team's pioneering efforts to apply quantum computing to a simplified portion of particle collider data are promising, Bauer said that he doesn't expect quantum computers to have a large impact on the high-energy physics field for several years – at least until the hardware improves.

Quantum computers will need more qubits and much lower noise to have a real breakthrough, Bauer said. "A lot depends on how quickly the machines get better." But he noted that there is a huge and growing effort to make that happen, and it's important to start thinking about these quantum algorithms now to be ready for the coming advances in hardware.

As hardware improves it will be possible to account for more types of bosons and fermions in the quantum algorithm, which will improve its accuracy.

Such algorithms should eventually have broad impact in the high-energy physics field, he said, and could also find application in heavy-ion-collider experiments.

Also participating in the study were Benjamin Nachman and Davide Provasoli of the Berkeley Lab Physics Division, and Wibe de Jong of the Berkeley Lab Computational Research Division.

This work was supported by the U.S. Department of Energy Office of Science. It used resources at the Oak Ridge Leadership Computing Facility, which is a DOE Office of Science user facility.

34 COMB: largest breach of all time leaked online with 3.2 billion records

by Bernard Meyer

https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/

It's being called the biggest breach of all time and the mother of all breaches: COMB, or the Compilation of Many Breaches, contains more than 3.2 billion unique pairs of cleartext emails and passwords. While many data breaches and leaks have plagued the internet in the past, this one is exceptional in the sheer size of it. To wit, the entire population of the planet is at roughly 7.8 billion, and this is about 40% of that.

However, when considering that only about 4.7 billion people are online, COMB would include the data of nearly 70% of global internet users (if each record was a unique person). For that reason, users are recommended to immediately check if their data was included in the leak. You can head over to the CyberNews personal data leak checker now.

CyberNews was the first leak database to include the COMB data. Since COMB was first released, nearly 1 million users have checked our personal data leak checker to see if their data was included in the biggest breach compilation of all time.

So how did the COMB data leak happen?

On Tuesday, February 2, COMB was leaked on a popular hacking forum. It contains billions of user credentials from past leaks from Netflix, LinkedIn, Exploit.in, Bitcoin and more. This leak is comparable

to the Breach Compilation of 2017, in which 1.4 billion credentials were leaked.

However, the current breach, known as "Compilation of Many Breaches" (COMB), contains more than double the unique email and password pairs. The data is currently archived and put in an encrypted, password-protected container.

The leaked database includes a script named count˙total.sh, which was also included in 2017's Breach Compilation. This breach also includes two other scripts: query.sh, for querying emails, and sorter.sh for sorting the data.

After running the count˙total.sh script, which is a simple bash script to count the total lines in each of the files and add them together, we can see there are more than 3.27 billion email and password pairs:

We are currently adding the new COMB emails to our Personal Data Leak Checker. The CyberNews Personal Data Leak Checker has the largest database of known breached accounts, helping users know if their data has possibly fallen into the hands of cybercriminals.

This does not appear to be a new breach, but rather the largest compilation of multiple breaches. Much like 2017's Breach Compilation, COMB's data is organized by alphabetical order in a tree-like structure, and it contains the same scripts for querying emails and passwords.

In the screenshots attached with the leak, the organization of the data can be seen, as well as the type of data released. Below, the data has been blurred by CyberNews:

At the moment, it is unclear what previously leaked databases are collected in this breach. Samples seen by CyberNews contained emails and passwords for domains from around the world.

11 Feb 2021

35 The First UK-US Signals Intelligence Cooperation

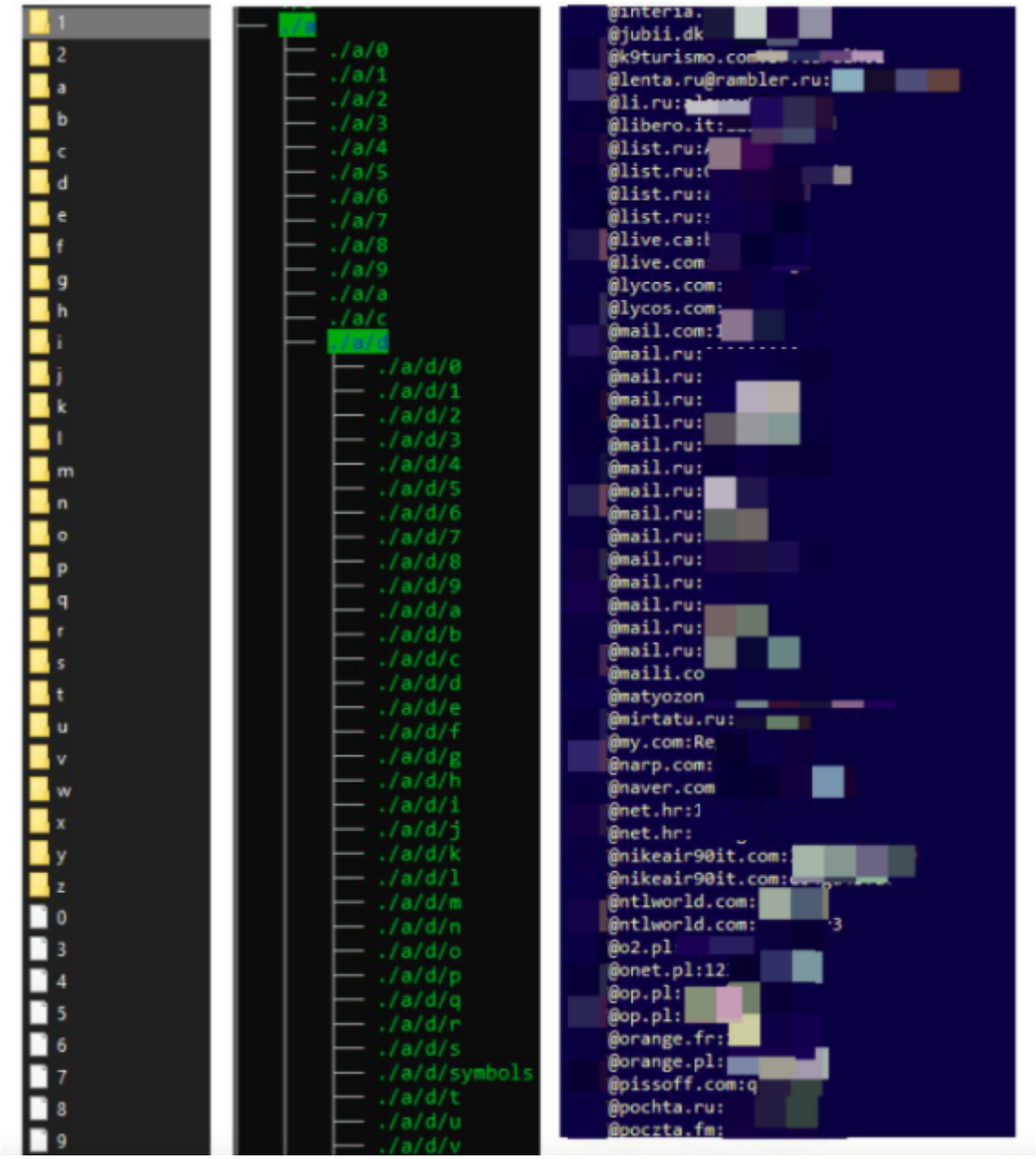
by NSA

https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2501548/the-first-uk-us-signals-intelligence-cooperation/

Before World War II, military education in the United States did not provide much instruction in intelligence. Gen. Dwight Eisenhower, as he rose to command, therefore had no formal education in it and little experience in using intelligence other than tactical methods, such as reconnaissance.

When Gen. Eisenhower became the senior U.S. officer in Europe in August 1942, Prime Minister Winston Churchill invited the American general to his weekend residence for a "get acquainted" visit. There, he personally briefed him on ULTRA, the exploitation of the German ENIGMA machine. Eisenhower became a skilled user of intelligence as the Allied Supreme Commander in Europe in World War II. But first he had to learn the challenging art of commanding armies from different military traditions and simultaneously learn to use intelligence.

Prior to taking command in Europe for the mission to liberate the countries occupied by the Nazis, Eisenhower led the first major binational military force in North Africa in late 1942, and appointed British Brigadier Kenneth Strong as his G-2, intelligence chief.


1
2
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z
0
3
4
5
6
7
8
9
./a/0
./a/1
./a/2
./a/3
./a/4
./a/5
./a/6
./a/7
./a/8
./a/9
./a/a
./a/c
./a/d/0
./a/d/1
./a/d/2
./a/d/3
./a/d/4
./a/d/5
./a/d/6
./a/d/7
./a/d/8
./a/d/9
./a/d/a
./a/d/b
./a/d/c
./a/d/d
./a/d/e
./a/d/f
./a/d/g
./a/d/h
./a/d/i
./a/d/j
./a/d/k
./a/d/l
./a/d/m
./a/d/n
./a/d/o
./a/d/p
./a/d/q
./a/d/r
./a/d/s
./a/d/symbols
./a/d/t
./a/d/u
@jubii.dk
@lenta.ru@rambler.ru:
@libero.it:
@live.com
@lycos.com:
@mail.ru:
@matyozon
@mirtatu.ru:
@naver.com
@net.hr:
@o2.pl
@onet.pl:12
@orange.fr:
@orange.pl:
@pissoff.com:q
@pocht a.ru:

Strong proved equally expert in getting along with the Americans as he was in intelligence analysis. He had worked in intelligence for almost seventeen years.

Strong worked so well with Eisenhower and the senior staff that Eisenhower asked to have the British officer again assigned to him when he was selected to command the cross-channel operation to land Allied forces in France, and moved his headquarters to London. Strong served with Eisenhower through the end of the war, and his tutelage on intelligence not only influenced General Eisenhower for the better but, of course, helped to educate the future President Eisenhower.

36 UMass Amherst Team Helps Demonstrate Spontaneous Quantum Error Correction

by Shiera D. Goff

https://www.umass.edu/newsoffice/article/umass-amherst-team-helps-demonstrate

To build a universal quantum computer from fragile quantum components, effective implementation of quantum error correction (QEC) is an essential requirement and a central challenge. QEC is used in quantum computing, which has the potential to solve scientific problems beyond the scope of supercomputers, to protect quantum information from errors due to various noise.

Published by the journal Nature, research co-authored by University of Massachusetts Amherst physicist Chen Wang, graduate students Jeffrey Gertler and Shruti Shirol, and postdoctoral researcher Juliang Li takes a step toward building a fault-tolerant quantum computer. They have realized a novel type of QEC where the quantum errors are spontaneously corrected.

Today's computers are built with transistors representing classical bits (0's or 1's). Quantum computing is an exciting new paradigm of computation using quantum bits (qubits) where quantum superposition can be exploited for exponential gains in processing power. Fault-tolerant quantum computing may immensely advance new materials discovery, artificial intelligence, biochemical engineering and many other disciplines.

Since qubits are intrinsically fragile, the most outstanding challenge of building such powerful quantum computers is efficient implementation of quantum error correction. Existing demonstrations of QEC are active, meaning that they require periodically checking for errors and immediately fixing them, which is very demanding in hardware resources and hence hinders the scaling of quantum computers.

In contrast, the researchers' experiment achieves passive QEC by tailoring the friction (or dissipation) experienced by the qubit. Because friction is commonly considered the nemesis of quantum coherence, this result may appear quite surprising. The trick is that the dissipation has to be designed specifically in a quantum manner. This general strategy has been known in theory for about two decades, but a practical way to obtain such dissipation and put it in use for QEC has been a challenge.

"Although our experiment is still a rather rudimentary demonstration, we have finally fulfilled this counterintuitive theoretical possibility of dissipative QEC," says Chen. "Looking forward, the implication is that there may be more avenues to protect our qubits from errors and do so less expensively. Therefore, this experiment raises the outlook of potentially building a useful fault-tolerant quantum computer in the mid to long run."

Chen describes in layman's terms how strange the quantum world can be. "As in German physicist Erwin Schrödinger's famous (or infamous) example, a cat packed in a closed box can be dead or alive at

the same time. Each logical qubit in our quantum processor is very much like a mini-Schrödinger's cat. In fact, we quite literally call it a 'cat qubit.' Having lots of such cats can help us solve some of the world's most difficult problems."

"Unfortunately, it is very difficult to keep a cat staying that way since any gas, light, or anything leaking into the box will destroy the magic: The cat will become either dead or just a regular live cat," explains Chen. "The most straightforward strategy to protect a Schrodinger's cat is to make the box as tight as possible, but that also makes it harder to use it for computation. What we just demonstrated was akin to painting the inside of the box in a special way and that somehow helps the cat better survive the inevitable harm of the outside world."

10 Feb 2021

37 Quantum effects help minimize communication flaws

by University of Vienna

https://phys.org/news/2021-02-quantum-effects-minimize-flaws.html

Noise limits the performance of modern quantum technologies. However, particles travelling in a superposition of paths can bypass noise in communication. A collaboration between the Universities of Hong-Kong, Grenoble and Vienna, as well as the Austrian Academy of Sciences, under the lead of Philip Walther, reveals novel techniques to reduce noise in quantum communication. The results, published in the latest issue of Physical Review Research, demonstrate that quantum particles travelling in a superposition of paths enable noise reduction in communications.

Among the most active fields of research in modern physics, both at an academic level and beyond, are quantum computation and communication, which apply quantum phenomena such as superposition and entanglement to perform calculations, or to exchange information. A number of research groups around the world have built quantum devices that are able to perform calculations faster than any classical computer. Yet, there is still a long way to go before these devices can be converted into marketable quantum computers. One reason for this is that both quantum computation and quantum communication are strongly deteriorated by the ease with which a quantum superposition state can be destroyed, or entanglement between two or more quantum particles can be lost.

The primary approach to overcome these limitations is the application of so-called quantum error-correcting codes. This, however, requires an amount of resources exceeding that which can be currently achieved in a controlled way. While, in the long run, error correction is likely to become an integral part of future quantum devices, a complementary approach is to mitigate the noise – that is, the cumulative effect of uncorrected errors – without relying on so many additional resources. These are referred to as noise reduction schemes.

Noise mitigation without additional resources through simple quantum schemes

A new approach along this research line was recently proposed to reduce noise in a communication scheme between two parties. Imagine two parties who want to communicate by exchanging a quantum particle, yet the particle has to be sent over some faulty transmission lines (depicted in the artistic illustration).

Recently, a team of researchers at Hong-Kong University proposed that an overall reduction in noise could be achieved by directing the particle along a quantum superposition of paths through regions of noise in opposite order. In particular, while classically a particle can only travel along one path, in quantum mechanics it can move along multiple paths at once. If one uses this property to send the particle along two quantum paths, one can, for instance, lead the particle across the noisy regions in opposite order simultaneously. This effect had been demonstrated experimentally by two independent research investigations.

These results suggested that, to achieve this noise reduction, it is necessary to place the noisy transmission lines in a quantum superposition of opposite orders. Shortly after this, research groups in Vienna and in Grenoble realized that this effect can also be achieved via simpler configurations, which can even completely eliminate the noise between the two parties.

All of these schemes have now been implemented experimentally and compared with each other by a research team led by Philip Walther at the University of Vienna. In this work, different ways of passing through two noisy regions in quantum superposition are compared for a variety of noise types. The experimental results are also supported with numerical simulations to extend the study to more generic types of noise. Surprisingly, it is found that the simplest schemes for quantum superposition of noisy channels also offer the best reduction of the noise affecting communication.

”Error correction in modern quantum technologies is among the most pressing needs of current quantum computation and communication schemes. Our work shows that, at least in the case of quantum communication, already with the technologies currently in use it may be possible to mitigate this issue with no need for additional resources,” says Giulia Rubino, first author of the publication in Physical Review Research. The ease of the demonstrated technique allows immediate use in current long-distance communications, and promises potential further applications in quantum computation and quantum thermodynamics.

38 china launches first quantum computer operating system to challenge us in technological ‘arms race’

by Anthony Cuthbertson

https://www.independent.co.uk/life-style/gadgets-and-tech/quantum-computing-china-us-arms-race-b1799611.html

A Chinese startup has launched the country’s first homegrown operating system for a quantum computer, challenging the dominance of the United States in the development of the next-generation machines.

Origin Quantum, based in the eastern province of Anhui, unveiled its Origin Pilot OS on Monday, according to local media, in what is the latest in a series of quantum computing breakthroughs coming out of China.

Quantum computers hold the potential to radically transform everything from space exploration to the curing and treatment of disease thanks to their vast power compared to current computing systems. Military uses for stealth aircraft and communications has led to warnings that quantum innovations could transform warfare, with leading computing commentator Martin Giles describing competition between the US and China as a “quantum arms race”.

Major advances in recent years have begun to see the first practical uses of the technology since it was

first theorised by the physicist Richard Feynman in 1982.

Research teams in both China and the US have achieved a milestone referred to as quantum supremacy, whereby a quantum computer performed a calculation that would have taken the world's most powerful supercomputer thousands of years to complete.

Quantum computers achieve their immense power by replacing traditional bits – the '1's' and '0's' used to store and transfer data – with qubits, which can function as both a '1' and a '0' at the same time by acting in a state of superposition.

This capability means that a quantum computer's processing power increases exponentially with each new qubit added, rather than linearly.

In order to harness this immense power, a functional operating system is required to act as a software interface for users to build practical applications.

"If the quantum chip is compared to the heart of a human, the quantum computer operating system is equivalent to the brain and the quantum application software is the flesh and blood," said Guo Guangcan from the Chinese Academy of Sciences.

The first operating system for a quantum computer was first developed by researchers in Cambridge in 2015, who claimed that its development was necessary to realise the "profound and far-reaching effects on a vast number of aspects of our daily lives."

Other systems have since been developed by researchers at Stanford University, paving the way for teams in the US to build next-generation applications for quantum computers.

The latest breakthrough in China comes as Origin Quantum secured additional funds in Series A funding from state-affiliated fund China Internet Investment Fund in its bid to close the gap to leading US players like Google and IBM.

The operating system will be used on a cloud platform to offer quantum computing capabilities to more than 100 companies that have already signed up.

39 Is Your Qubit Better Than My Qubit?

by Corey Rae McRae

https://www.nist.gov/blogs/taking-measure/your-qubit-better-my-qubit

I had been studying superconducting quantum computing for seven years before I was stumped by this seemingly simple question: How do I know if my qubit is better than your qubit?

Quantum computers could ultimately unlock the capability to solve hard problems in chemistry, cryptography and quantum mechanics. Researchers around the world are pursuing numerous designs for quantum computers, including qubits, or quantum bits, that serve as the basic building block of these computers. Google and IBM, among others, create qubits using superconducting materials, which have special properties, including the ability to conduct electricity without resistance. Quantum computers based on superconducting qubits show great promise toward achieving large-scale computing power.

Qubits are the fundamental component of quantum processors, and their performance can dictate the processing power. But determining just how "good" a qubit is can be a problem in and of itself. This question led me down a research rabbit hole that could revolutionize the way researchers improve quantum

computers, and could ultimately unlock the capability to solve hard, field-defining problems in chemistry, cryptography and quantum mechanics.

In graduate school at the University of Waterloo in Canada, I focused my studies on measuring the performance of different materials in the extremely cold, low-power environment used to operate superconducting quantum computers. Superconducting quantum circuits require a temperature of around one hundredth of a degree above absolute zero, as well as around one photon of average power for optimal operation. This requires the use of ultralow-temperature refrigerators and complex electrical setups using microwave frequencies.

During my graduate research, I studied different types of superconducting aluminum and indium and compared the results to determine which ones made better or worse devices. But a concern always plagued me: Device performance seemed to vary significantly based on small changes we made when setting up the experiment and analyzing the data, and even over time! Later, I learned that these apparent performance fluctuations are a major issue in the implementation of multiqubit algorithms such as the IBM Q processors.

So, with all these different fluctuations in play, how can I tell if my qubit with niobium wiring is better than your qubit with aluminum wiring? Without this ability, we can't make the many small improvements we need to optimize our circuits, and we are stuck trying to make dramatic, moonshot changes, which are rare and hard to achieve.

This is where the Boulder Cryogenic Quantum Testbed comes into play. I founded the testbed at the University of Colorado Boulder along with David Pappas, leader of the Quantum Processing Group at the National Institute of Standards and Technology (NIST), and Josh Mutus, a research scientist at Google. It is a highly collaborative laboratory with a one-of-a-kind experimental setup for accurate measurement of superconducting quantum circuits. We measure superconducting devices from academic, industry and national labs, as well as devices fabricated at NIST from novel materials such as gallium arsenide, and carefully analyze the data to extract their performance in a reproducible manner. Using our setup and analysis, we can account for many of the performance variations seen and not only accurately compare device performance, but also come to a fuller understanding of the sources of these fluctuations in performance.

By taking advantage of NIST's leading expertise in metrology, the Boulder Cryogenic Quantum Testbed has become a driving force in the study of qubit performance. We expect this effort to lead to never-before-seen high-performance devices and, eventually, a full-scale quantum computer with the power to revolutionize humanity's capability to solve hard problems.

09 Feb 2021

40 Brazil Quantum: A pioneering initiative

https://www.swissquantumhub.com/brazil-quantum-a-pioneering-initiative/

By the beginning of 2020, no initiatives were promoting and discussing quantum technologies outside the academia in Brazil. Also, unlike many developed countries, Brazil has not defined a national plan to develop Quantum Computing. There was an urge for someone to take action and to start this movement among Brazilians.

A group of four friends had decided to take this responsibility and founded Brazil Quantum, with the

ultimate goal to make Brazil a global player in quantum computing. Rodrigo Ferreira, Pedro Ripper, Rafael Verissimo, and Camila Pontes started as an online community (to connect students and enthusiasts) and a blog page (to promote and explain the basics of quantum computing).

The initiative has substantially grown over time and started to perform different activities. Beyond the online community – which has expanded to a couple of hundred members – and the blog page, Brazil Quantum also runs an interview series in which experts come to talk about their research. The real impact, however, was yet to come.

Brazil Quantum began to explore real use cases to quantum computing technology. The first case is a post-quantum cryptography study in partnership with the Central Bank of Brazil and supported by Microsoft. This study is supervised by the Central Bank's Information Technology Department (DEINF), which has been leading innovative studies and projects, such as central bank digital currencies (CDBC) and the Brazilian instant payment system (PIX).

Our current initiative focuses on PIX (Central Bank of Brazil's instant payments ecosystem), a widely used platform that has moved BRL 83.4 billion in only one month. Brazil Quantum is analyzing and comparing the main quantum-safe algorithms to evaluate the feasibility of their use in a retail instant payment system, like PIX. The proof of concept will culminate into a paper that will discuss the quantum-safe algorithms' applicability and scalability on PIX.

Not limited to post-quantum cryptography, Brazil Quantum is developing one of the firsts introductory quantum computing courses in Portuguese with its partner QURECA (Quantum Resources and Careers). The initiative believes that this course can motivate young students to pursue their future studies and push the Brazilian quantum workforce forward.

Moreover, the initiative is also pairing up with the Applied Artificial Intelligence Institute (I2A2) to create a quantum computing course series in English. The first part is about theory and programming basics, while the second will focus on a specific field of quantum technologies. The enrolled students must complete tasks throughout the course to save their spot in the cohort and ultimately earn the completion certificate.

Beyond those educational resources, Brazil Quantum is negotiating a study project with Klabin S.A. – the largest paper producer, exporter, and recycler in Brazil – on behalf of Arnaldo Gunzi (Klabin's project manager). A couple of interns will be selected to study and propose an approach to an optimization problem via quantum algorithms. As that will be one of the firsts quantum-based projects on the Brazilian industry in general, Brazil Quantum and Klabin are confident that it might attract other companies into this field.

41 New quantum algorithm verifying Quantum Advantage in seconds

https://www.swissquantumhub.com/new-quantum-algorithm-verifying-quantum-advantage-in-seconds/

CNRS (Centre National de Recherche Scientifique/The French National Center for Scientific Research) announced today that scientists from CNRS, the University of Edinburgh, and QC Ware have successfully demonstrated that a quantum machine using a new quantum algorithm can verify quantum advantage in seconds, while a classical computer can take thousands of years to perform the same task.

Iordanis Kerenidis, Senior Researcher, CNRS, and Head of Algorithms – International, QC Ware, is co-author of the research paper. The leading quantum algorithms expert conceived the project, designed the algorithm, and analyzed its performance.

The experiment focused on verifying NP-complete problems using only a small and unverified slice of information. It implemented Kerenidis' complex, interactive, algorithm which enabled a great reduction in quantum hardware requirements and the use of a simple, experimental, photonic system comprising two laser sources, a single-beam splitter, and two detectors.

NP-complete problems refer to a large variety of the most significant computational problems in industry in a range of fields including manufacturing optimization, machine learning, server-client quantum computing, authentication systems, and blockchain technologies.

The top-speed quantum verification of such problems can open the way for trusted quantum cloud computing. Without gaining insight into a cloud quantum provider's full quantum solutions, clients can verify or validate claims such as portfolio optimization with much higher returns or machine learning models with much higher accuracy.

42 Solving the Cryptography Riddle: Post-quantum Computing & Crypto-assets Blockchain Puzzles

https://www.enisa.europa.eu/news/enisa-news/solving-the-cryptography-riddle-post-quantum-computing-crypto-assets-blockchain-puzzles

Cryptography is a vital part of cybersecurity. Security properties like confidentiality, integrity, authentication, non-repudiation rely on strong cryptographic mechanisms, especially in an always connected, always online world.

In addition, cryptography's applications open up new opportunities and markets: digital signatures or online transactions would not be possible without it. Given its importance, cryptography (encryption) remains a heavily researched field, and even finds its way into the headlines, referred to in high level documents and even legislation.

One such document is the new EU Cybersecurity Strategy (December 2020), which mentions out quantum computing and encryption as key technologies for achieving resilience, technological sovereignty and leadership.

With the objective to support the implementation of the Cybersecurity Strategy and of relevant legislative efforts, ENISA publishes two reports on the topic of cryptography. The first one focuses on the forthcoming disruptions of post-quantum computing on our present cybersecurity infrastructure and how we need to mitigate it. The second one introduces the cryptographic building blocks used in a majority of digital currencies & crypto-assets, which will fall under the scope of a new EU regulatory proposal.

Post Quantum security and why it matters

Quantum technology will enable a huge leap forward in many branches of industry, as it can efficiently resolve problems technologies of today are not able to provide a solution for. However, this technology will be highly disruptive for our current security equipment and systems.

As a matter of fact, scientists commonly agree that quantum computers will be able to break widely used public-key cryptographic schemes. These are the same schemes working behind the green lock in our browser tabs telling us that our data are protected against malicious eavesdroppers. Similarly, these are also the same schemes allowing us to have digital signatures and designed to implement the Electronic identification (eID) and Trust Services of the eIDAs regulation. Consequently, data or processes protected

by those schemes, such as bank transactions, software updates, digitally signed official documents, patient records and more, will instantly cease to be secure.

This initiative is motivated by the fact that the transition to new quantum resistant cryptographic algorithms will take years, since the related processes are both extremely intricate and financially costly.

The study – Post-Quantum Cryptography: Current state and quantum mitigation – provides a concise overview of the current progress of the standardisation process of post-quantum cryptography (PQC) schemes. It introduces a framework to analyse existing quantum-safe solutions, classifying them into families and discussing their advantages and shortcomings.

With contributions from top experts in the field, it helps readers navigate an overly complex but also fascinating topic for the future of cybersecurity. The study aims to help decision makers and system designers take up appropriate actions, as soon as possible. To that end, it includes useful quantum resistant techniques that can be implemented in today's systems until PQC algorithms become standardised and generally available.

Under the hood of crypto assets & the Distributed Ledger Technology

With the creation of a pan-European blockchain regulatory sandbox, the European Union intends to put Distributed Ledger Technologies (DLTs) to the test. Such technologies, also referred to as blockchain technologies, are those on which digital assets such as cryptocurrencies are built upon. But the applications do not stop there, smart contracts, anti-counterfeit seals, even games, have been based on a few important cryptographic building blocks.

The ENISA report – Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies – aims to further increase understanding around these underlying cryptographic components that compose the blockchain and in extension crypto-assets, digital currencies and the host of applications possible.

As a continuation of an earlier report on the security and challenges of DLTs, this report provides an in-depth explanation of the technical components involved and illustrates their uses into popular deployed instances.

By focusing on crypto-assets, ENISA intends to support policymakers by explaining the underling cryptographic mechanics used and raise awareness on foreseen security, financial, legal and data protection issues.

Background

This work falls under the provisions of Articles 5, 8, 9 and 11 of the Cybersecurity Act. ENISA's Work Programme foresees activities to support Knowledge Building in Cryptographic algorithms.

In cooperation with the European Commission, Member States and other EU bodies, the Agency engages with expert groups to address emerging challenges and promote good practices.

One of these emerging risks arise in relation to quantum computing cryptanalytics capabilities, where there is need to transition to quantum safe encryption as a counter measure and to support EU in advancing its strategic digital autonomy. In addition, the continuation of past ENISA work on blockchain security with a new study looking at the cryptographic components was very timely as it coincided with the EU efforts in regulating crypto-assets and the announcement of the ECB that it is exploring the plausibility of a centrally backed digital euro, to complement the euro banknote.

08 Feb 2021

43 Scientists create armour for fragile quantum technology

by FLEET

https://phys.org/news/2021-02-scientists-armour-fragile-quantum-technology.html

An international team of scientists has invented the equivalent of body armour for extremely fragile quantum systems, which will make them robust enough to be used as the basis for a new generation of low-energy electronics.

The scientists applied the armour by gently squashing droplets of liquid metal gallium onto the materials, coating them with gallium oxide.

Protection is crucial for thin materials such as graphene, which are only a single atom thick – essentially two-dimensional (2-D) – and so are easily damaged by conventional layering technology, said Matthias Wurdack, who is the lead author of the group's publication in Advanced Materials.

"The protective coating basically works like a body armour for the atomically-thin material, it shields against high-energy particles, which would cause a large degree of harm to it, while fully maintaining its optoelectronic properties and its functionality," said Mr Wurdack, a Ph.D. student in the Nonlinear Physics Centre (NLPC) of the Research School of Physics, and the FLEET ARC Centre of Excellence.

The new technique opens the way for an industry based on ultra-thin electronics to expand, said leader of the research team, Professor Elena Ostrovskaya, also from NLPC and FLEET.

"Two-dimensional materials have extraordinary properties such as extremely low resistance or highly efficient interactions with light."

"Because of these properties they could have big role in the fight against climate change."

Eight percent of global electricity consumption in 2020, was due to information technologies, including computers, smartphones and large data centres of tech giants such as Google and Amazon. That figure is projected to double every decade as demand for AI services and smart devices skyrockets.

However, this work promises lower-energy alternatives for electronics and optoelectronics, by harnessing the superior performance of 2-D semiconducting materials, such as tungsten disulphide, which was used in this study.

Using 2-D materials to make more efficient devices will have advantages beyond reduced carbon emissions, says Mr Wurdack.

"2-D technology could also enable super-efficient sensors on space craft, or processors in Internet of Things devices that are less limited by battery life."

The team created their protective layer by exposing to air a droplet of liquid gallium, which immediately formed a perfectly even layer of gallium oxide on its surface a mere three nanometers thick.

By squashing the droplet on top of the 2-D material with a glass slide, the gallium oxide layer can be transferred from the liquid gallium onto the material's entire surface, up to centimetres in scale.

Because this ultrathin gallium oxide is an insulating amorphous glass, it conserves the optoelectronic properties of the underlying 2-D semiconductor. The gallium oxide glass can also enhance these properties

at cryogenic temperatures and protects well against other materials deposited on top. This allows the fabrication of sophisticated, layered nanoscale electronic and optical devices, such as light emitting diodes, lasers and transistors.

"We've generated a nice alternative to existing technology that can be scaled for industry applications," Mr Wurdack said.

"We hope to find industry partners to work with us to develop a protective layer printer based on this technology, that can go into any lab, like a lithography machine."

"It would be exciting to see fundamental research like this find its way into industry!"

06 Feb 2021

44 Hackers leak Army personnel's data using Airtel network, telco denies any breach

by PTI

https://www.businesstoday.in/current/economy-politics/hackers-leak-army-personnel-data-using-airtel-network-telco-denies-any-breach/story/430497.html

A hacker group has allegedly leaked data of Army personnel using Bharti Airtel network in Jammu and Kashmir, however, the company has denied any breach in its system.

The group, with the name of Red Rabbit Team, hacked some Indian websites and posted the data on the web pages of those portals.

The hackers shared some links of those web pages on Twitter in a comment over a tweet of cyber security researcher Rajshekhar Rajaharia and tagged several media organisations.

The query sent to the Indian Army did not elicit any reply but an Army official said "We are not aware of any such information but it appears to be malicious intent of some inimical elements".

When contacted, Bharti Airtel spokesperson denied any breach of its server.

"We can confirm there is no hack or breach of any Airtel system as claimed by this group. Multiple stakeholders outside of Airtel have access to some data as per regulatory requirements. We have apprised all the relevant authorities of the matter to, therefore, investigate this and take appropriate action."

"This group has been in touch with our security team for over 15 months now and has made varying claims in addition to posting inaccurate data from one specific region," the spokesperson said.

The links shared by the hacker were initially accessible with mobile number, name and address of subscribers but stopped working after sometime.

Red Rabbit Team in a message to PTI claimed that it has access to pan-India data of Bharti Airtel through a shell uploaded on the company's server and will leak more data soon.

Rajaharia said that hackers have failed to show any credible evidence of possessing pan-India data of Bharti Airtel and it is also unclear on the way they got subscriber's data.

"The hacker group failed to show evidence that they have a whole India database. Their claim of shell upload may be also fake. The video of SDR portal seems real but only a short portion of data may leak via this. It is still unclear how they got access to whole Jammu and Kashmir subscriber data," he said.

Telecom operators are required to give access to government and law enforcement agencies of subscriber data registration (SDR) portal through which phone numbers and subscribers details can be verified.

Rajaharia said that hackers may be from Pakistan.

"The website which was used to upload alleged Airtel data was hacked on December 4, 2020 by Mr Clay (TeamLeets – a Pakistani Hacker Group). This indicates that a Pakistani hacker group TeamLeets may be behind this data leak," Rajaharia said.

05 Feb 2021

45 Machine Learning helps Quantum Key Distribution

https://www.swissquantumhub.com/machine-learning-helps-quantum-key-distribution/

Continuous-Variable Quantum Key Distribution (CV-QKD) enables information-theoretically secure key exchange between two parties using the continuous-variable properties of the quantized electromagnetic light field.

The secret key rate of a CV-QKD system is limited by excess noise. A key issue typical to all modern CV-QKD systems implemented with a reference or pilot signal and an independent local oscillator is controlling the excess noise generated from the frequency and phase noise accrued by the transmitter and receiver.

Therefore accurate phase estimation and compensation, so-called carrier recovery, is a critical subsystem of CV-QKD.

Researchers have explored the implementation of a Machine Learning (ML) framework based on Bayesian inference, namely an Unscented Kalman Filter (UKF), for estimation of phase noise and compare it to a standard reference method and a previously demonstrated machine learning method.

Experimental results obtained over a 20-km fibre-optic link indicate that the UKF can ensure very low excess noise even at low pilot powers. The measurements exhibited low variance and high stability in excess noise over a wide range of pilot signal to noise ratios.

This may enable CV-QKD systems with low hardware implementation complexity which can seamlessly work on diverse transmission lines.

46 Quantum systems learn joint computing

by Max-Planck-Institut für Quantenoptik

https://phys.org/news/2021-02-quantum-joint.html

Today's quantum computers contain up to several dozen memory and processing units, the so-called qubits. Severin Daiss, Stefan Langenfeld, and colleagues from the Max Planck Institute of Quantum Optics in Garching have successfully interconnected two such qubits located in different labs to a distributed quantum computer by linking the qubits with a 60-meter-long optical fiber. Over such a distance they realized a quantum-logic gate – the basic building block of a quantum computer. It makes the system the worldwide first prototype of a distributed quantum computer.

The limitations of previous qubit architectures

Quantum computers are considerably different from traditional "binary" computers: Future realizations of them are expected to easily perform specific calculations for which traditional computers would take months or even years – for example in the field of data encryption and decryption. While the performance of binary computers results from large memories and fast computing cycles, the success of the quantum computer rests on the fact that one single memory unit – a quantum bit, also called "qubit" – can contain superpositions of different possible values at the same time. Therefore, a quantum computer does not only calculate one result at a time, but instead many possible results in parallel. The more qubits there are interconnected in a quantum computer; the more complex calculations it can perform.

The basic computing operations of a quantum computer are quantum-logic gates between two qubits. Such an operation changes – depending on the initial state of the qubits – their quantum mechanical states. For a quantum computer to be superior to a normal computer for various calculations, it would have to reliably interconnect many dozens, or even thousands of qubits for equally thousands of quantum operations. Despite great successes, all current laboratories are still struggling to build such a large and reliable quantum computer, since every additionally required qubit makes it much harder to build a quantum computer in just one single set-up. The qubits are implemented, for instance, with single atoms, superconductive elements, or light particles, all of which need to be isolated perfectly from each other and the environment. The more qubits are arranged next to one another, the harder it is to both isolate and control them from outside at the same time.

Data line and processing unit combined

One way to overcome the technical difficulties in the construction of quantum computers is presented in a new study in the journal Science by Severin Daiss, Stefan Langenfeld and colleagues from the research group of Gerhard Rempe at the Max Planck Institute of Quantum Optics in Garching. In this work supported by the Institute of Photonic Sciences (Castelldefels, Spain), the team succeeded in connecting two qubit modules across a 60-meter distance in such a way that they effectively form a basic quantum computer with two qubits. "Across this distance, we perform a quantum computing operation between two independent qubit setups in different laboratories," Daiss emphasizes. This enables the possibility to merge smaller quantum computers to a joint processing unit.

Simply coupling distant qubits to generate entanglement between them has been achieved in the past, but now, the connection can additionally be used for quantum computations. For this purpose, the researchers employed modules consisting of a single atom as a qubit that is positioned amidst two mirrors. Between these modules, they send one single light quanta, a photon, that is transported in the optical fiber. This photon is then entangled with the quantum states of the qubits in the different modules. Subsequently, the state of one of the qubits is changed according to the measured state of the "ancilla photon," realizing a quantum mechanical CNOT-operation with a fidelity of 80%. A next step would be to connect more than two modules and to host more qubits in the individual modules.

Higher performance quantum computers through distributed computing

Team leader and institute director Gerhard Rempe believes the result will allow to further advance the technology: "Our scheme opens up a new development path for distributed quantum computing." It could enable, for instance, to build a distributed quantum computer consisting of many modules with few qubits

that are interconnected with the newly introduced method. This approach could circumvent the limitation of existing quantum computers to integrate more qubits into a single setup and could therefore allow more powerful systems.

47 Security Threats of Quantum Technologies and Ways to Overcome Them

by David Balaban

https://thequantumdaily.com/2021/02/05/security-threats-of-quantum-technologies-and-ways-to-overcome-them/

The natural acceleration of technological evolution provides humans with new opportunities, paving the way toward a future that seemed to be science fiction only a few years ago. That said, ground-breaking technologies that will be adopted dData line and processing unit combinedown the road will give rise to equally revolutionary threats. These concerns require an all-new approach to security and collective solutions that should be implemented on a global scale.

The computation speed of quantum computers is multiple orders of magnitude higher than that of their classic counterparts. Not only does this save a ton of time when processing the most complex tasks, but it also calls forth new threats in areas like cryptography.

The progress of quantum technology could transform society and multiple industries. Businesses and governments should accurately assess the scale of the phenomenon along with the associated risks and start building quantum security. To unleash the full power of this promising tech, decision-makers need to address the distributed and systemic risks that require collective action and solutions.

The quantum arms race

Quantum computing systems are capable of completing data processing tasks traditional computers cannot handle. In the next 5-15 years, such machines will underlie a strategically important technology potent enough to become a foundation for a new technological revolution.

Nowadays, researchers are solving complex engineering problems to create hardware and software that will allow the theoretical potential of quantum computing to be put into practice. Forecasts regarding the practical uses of the technology vary. It is generally believed that mankind will see the first real-world results within a decade.

However, these could be pessimistic predictions as significant funds from corporations and governments are being invested into the development process. The potential trillions of dollars in profits set a technological arms race in motion.

Quantum algorithms will be able to perform simulations at the molecular level, accelerating the discovery of new drugs and high-tech materials. The unprecedented computing speed will optimize the finance sector and the aerospace industry, opening new horizons for the potential of artificial intelligence (AI).

A small range of companies is already offering pilot versions of quantum computing services. These projects encourage customers to combine efforts with developers and create the algorithms required to fully implement the tech in a target sector.

The benefits are already attainable or will become attainable soon. The progress stemming from the evolution of quantum computers has not been fully converted to practical applications. But it is already clear that not only companies, but entire nation-states may fall behind the mind-boggling progress some will achieve.

Cryptographic risk – the least of all evils

The global cybersecurity community is already seeing the challenges associated with the quantum arms race. Here is a rundown on these roadblocks.

- **Violation of the cryptographic infrastructure.** Quantum computers boast data processing speeds that pose a risk to asymmetric encryption, which currently underlies the security of numerous digital processes. Quantum-safe solutions are emerging that are not susceptible to this issue as they leverage post-quantum cryptography. Nevertheless, a number of implementation problems have yet to be addressed. The balance could be ruined if quantum computing becomes the privilege of a few individual members of the ecosystem. In this scenario, everyone else will be unable to ensure the confidentiality, integrity, and availability of their data.
- **Harvest now, decrypt later.** This risk applies to data and systems that stay unaltered over time and inherently have a long service life, such as satellites and certain kinds of transport. Threat actors can collect data from these entities now and decrypt it in the future. They could also sell this information to interested parties who have already mastered quantum technology.
- **Geopolitical risks and equal access.** The competitive advantages of quantum computing can deteriorate international relations, thus posing geopolitical risks. The accessibility of the technology to some countries and the "quantum poverty" of others may become serious obstacles to unlocking the potential of quantum computing.
- **New and secondary risks.** These are related to the adoption of this technology in various sectors. For instance, malefactors may interfere with algorithms and leave backdoors when the technology is being implemented – this way, they will be able to control it later for their own benefit. Computational power can become the pivot of new cyber-attack vectors or be used to mastermind pathogens, viruses, bioweapons that may create disruptive economic advantages in the global markets.

Required security solutions

Quantum computing could have a jaw-dropping potential in the cybersecurity context. Although some players in this ecosystem have not added quantum risks to their security equation yet, the appropriate protection solutions are already taking shape.

However, companies and officials need to take more effort in this regard. Businesses will have to understand and properly evaluate risks related to quantum security. The most significant components of this process are as follows:

- Acknowledgment of quantum risks to the company's infrastructure as well as an inventory of critical data assets.
- Professional management of the company's encrypted data and a roadmap for switching to quantum-safe cryptography.

- Staying on top of the emerging vulnerabilities that can be exploited by attackers with quantum computing power at their disposal. Security controls that hinge on computing resources are particularly important.
- Understanding the dependencies on partners, suppliers, and B2B services.
- Realizing the benefits of embedding quantum computing into the company's business model along with the potential risks of this shift.

Organizations should nurture the quantum literacy of their employees and senior management alike. This will play an important role in accurately assessing security risks and funding the quantum security department at a decent level.

Let us now go over some key quantum computing security issues and applicable solutions.

- **Distributed risk.** Shared infrastructures and interdependent sectors of the ecosystem require collective action to ensure quantum security. In some cases, these initiatives will need to be coordinated among multiple parties.
- **Safe quantum development practices.** Not only is this about educating qualified personnel with a profound understanding of the technology's complexity, but it is also about permanently refining the knowledge and qualifications to properly evaluate the security risks at all tiers and fend off malware attacks.
- **Management principles.** Standards and regulations are required to ascertain that companies assess risks in the quantum security arena. The same goes for decisions at the level of governments and regulatory authorities that should encourage companies to respond to the quantum threat adequately. International technical standards also need to be developed to eliminate barriers to further coordinated action. The ethical use of quantum computing is another growing issue that is escalating as the technology evolves. In this regard, the experience gained in international regulation of AI development could come in handy.
- **Equal access.** To avoid a technology gap between countries and to balance the benefits of quantum computing across the board, governments will need to team up. Consensual equal access to the technology will release its full potential and provide maximum security for all participants in the ecosystem in the face of potential cyber threats of the quantum future.

Takeaways

Today's global cybersecurity level is far from being perfect, but it suffices to maintain stability and avoid catastrophic consequences if failures happen. This may change in the near future, though. The development and implementation of quantum computing, artificial intelligence algorithms, and other sophisticated systems, as well as the growing complexity of network infrastructures and the interdependence of different sectors, will give rise to new systemic issues and risks. In such a paradigm, a security incident in one part of the system can impact the operation of another.

To steer clear of critical problems, all players in the dynamic cyberspace need to cooperate more tightly to reach a whole new level of security. The right time to start doing it is now. Not only do some technologies unearth information security issues of the future, but they also underlie ethical dilemmas that require careful discussion and regulation today.

04 Feb 2021

48 Cambridge Quantum Computing releases tket v0.7 with open access to all Python users

by Veronica Combs

https://www-techrepublic-com.cdn.ampproject.org/c/s/www.techrepublic.com/google-amp/article/cambridge-quantum-computing-releases-tket-v0-7-with-open-access-to-all-python-u

Cambridge Quantum Computing announced today that it has lifted licence restrictions on the Python module in the latest version of its quantum software development kit. Tket (pronounced "ticket") is an architecture agnostic quantum software stack and compiler.

Pytket, the Python module, interfaces with tket. This latest release allows any Python user with access to a quantum computer to deploy the tket SDK in any commercial or research contexts.

Mehdi Bozzo-Rey, head of business development at Cambridge Quantum Computing, said in a press release that the company hopes to accelerate the development of quantum computing research and applications across multiple industries by providing free access to the tket SDK to Python users across the world.

"By increasing the number of tket-compatible cloud-based quantum computing platforms as well, we've made it easier for virtually any programmer to explore developing quantum algorithms and software," he said.

Tket translates machine-independent algorithms into executable circuits and optimizes for physical qubit layout while also reducing the number of required operations. According to Cambridge Quantum Computing, tket allows collaborators and clients to work across several platforms and is applicable for problems in chemistry, material science, finance, and optimization. This set of tools supports circuits and device architectures from Google Cirq, IBM Qiskit, AQT, Honeywell, Amazon Braket, QSharp, Pyzx, ProjectQ, Qulacs, Rigetti pyQuil, and IonQ.

Tckt v0.7 also enables quantum circuit execution on Microsoft Azure Quantum (public preview version), and extends classical control of quantum operations on ion trap systems from Honeywell Quantum Solutions.

Tket allows users to migrate between devices by changing just a single line of code, according to the company. CQS also states that tket is used by many quantum hardware providers and major companies.

Other new features in the v0.7 release of tket include:

- Improved circuit optimization and noise mitigation performance with new methods to make constructing quantum circuits easier
- Substitution of named operations with other operations, boxes, or circuits
- Support for mid-circuit measurement on IBM Quantum premium devices

This new tool in the Python toolkit reflects an increasing interest in the language. Developers are more interested in learning to use that language than any other, according to a report from O'Reilly. As Lance Whitney reported on TechRepublic, interest in this language is up 27% over the previous year based

on findings in the report, "Where Programming, Ops, AI, and the Cloud are Headed in 2021." O'Reilly analyzed data from its online learning, publishing partners and learning modes, live online training courses, and virtual events to measure interest levels. Python is also desired for its machine learning (ML) aspects. The language's scikit-learn ML library saw an 11% increase in use, while the PyTorch ML framework used for deep learning jumped in use by 159%.

49 Safer Internet Day 2021: Here's how you can ensure your online security

by Cyrus John

https://www.bgr.in/how-to/here-are-some-step-to-help-you-stay-safe-while-browsing-the-internet-938145/

The world celebrates Safer Internet Day on 9 February every year by spreading awareness on how to prepare and react when faced with cyber threats. Several organisations globally make aware its employees and users about safeguards they need to follow while facing such threats online.

Yes, the internet can be fascinating but at the same time, it brings with it some challenges where we as users need to ensure that our identity and data online remains safe.

Apart from social media applications we also use a lot of banking and financial platforms on the internet which can be targeted by hackers.

Therefore, it is our responsibility to protect our identity and investments alike. So here are some ways you can ensure that your internet surfing experience is secure and you are safe from prying eyes.

- **Change your passwords regularly**

  I know it can be a task to have different passwords for different apps and services considering there are so many out there today but it is always a healthy practice to keep changing your passwords.

  It's hard to believe but there are still many internet users today who use '12345' as a password (ill-advised) and many use weak passwords for their social media accounts. So weak that even a monkey would be able to hack your account.

  - You should never use the same password for multiple apps and websites and
  - You should always use special characters while choosing a password.

  The more special characters mean the harder they are to crack. In case it's difficult for you to manage multiple passwords, get a password manager.

- **Using Incognito Mode while browsing**

  Nothing defines privacy more than the following: 'Ctrl+Shift+N'.

  The incognito mode on the web browser has been a bliss for internet users who want to keep their browsing private. For the uninitiated, **Incognito Mode** can be activated on multiple browsers like Google Chrome, Microsft Edge and Firefox but hitting the Ctrl+Shift+N keys or Command+Shift+N keys

  In Incognito Mode, your history, temporary internet files, or cookies are not stored on the computer. This also ensures that third-party websites and apps cannot track your online activity. Makes sure what's private, stays private.

- **Avoid using free Wi-Fi**

  We all love freebies. And if you are getting access to free internet, you've hit jackpot, right? Wrong.

  As hard as it might sound, using free Wi-Fi can mean trouble for your privacy and data security. You see hackers have their eyes set on these public networks and constantly hunt for weaknesses amidst its users. Since you have a lot of sensitive information on your phones and laptops you should avoid connecting your device to free Wi-Fi points.

- **Turn off location tracking on social media apps**

  There are several apps out there that unnecessarily track your location even if the app doesn't require it. If you come across such apps online it is advised that you deny location access to such apps. You also need to make sure that you deny location access to you social media websites like Facebook (unless you don't want to use its location-based services).

  Little do people know that even some web browsers ask for location access from users which is why you need to explore the Settings tab on your web browser and disable location access.

- **Use a VPN (Virtual Private Network)**

  When we say "Use a VPN" we meant the ones you can trust. There are several free VPNs out there but they come loaded with ads and at times malware.

  Most paid VPNs are bug-free and trustworthy. A VPN can boost your online security as it not only gives the user anonymity by creating a private network from a public connection but also assigns us another IP address so that our online activity cannot be traced.

- **Don't click everything**

  This is for those who cannot spot the difference between a download button and spam. Most hackers use scams to dupe people online. This can be done by sending fake emails and links that promise a cash reward or maybe even an exotic holiday. They can even be disguised as download links for software or images.

  Never trust such emails or invitations sent to your inbox as these might be malware that can be used to hack into your computer to steal sensitive financial information. You also should not click random download links on a website and double-check before you click on a link.

50 New quantum receiver the first to detect entire radio frequency spectrum

by The Army Research Laboratory

https://phys.org/news/2021-02-quantum-entire-radio-frequency-spectrum.html

A new quantum sensor can analyze the full spectrum of radio frequency and real-world signals, unleashing new potentials for soldier communications, spectrum awareness and electronic warfare.

Army researchers built the quantum sensor, which can sample the radio-frequency spectrum – from zero frequency up to 20 GHz – and detect AM and FM radio, Bluetooth, Wi-Fi and other communication signals.

The Rydberg sensor uses laser beams to create highly-excited Rydberg atoms directly above a microwave circuit, to boost and hone in on the portion of the spectrum being measured. The Rydberg atoms are sensitive to the circuit's voltage, enabling the device to be used as a sensitive probe for the wide range of signals in the RF spectrum.

"All previous demonstrations of Rydberg atomic sensors have only been able to sense small and specific regions of the RF spectrum, but our sensor now operates continuously over a wide frequency range for the first time," said Dr. Kevin Cox, a researcher at the U.S. Army Combat Capabilities Development Command, now known as DEVCOM, Army Research Laboratory. "This is a really important step toward proving that quantum sensors can provide a new, and dominant, set of capabilities for our Soldiers, who are operating in an increasingly complex electro-magnetic battlespace."

The Rydberg spectrum analyzer has the potential to surpass fundamental limitations of traditional electronics in sensitivity, bandwidth and frequency range. Because of this, the lab's Rydberg spectrum analyzer and other quantum sensors have the potential to unlock a new frontier of Army sensors for spectrum awareness, electronic warfare, sensing and communications – part of the Army's modernization strategy.

"Devices that are based on quantum constituents are one of the Army's top priorities to enable technical surprise in the competitive future battlespace," said Army researcher Dr. David Meyer. "Quantum sensors in general, including the one demonstrated here, offer unparalleled sensitivity and accuracy to detect a wide range of mission-critical signals."

The peer-reviewed journal Physical Review Applied published the researchers' findings, Waveguide-coupled Rydberg spectrum analyzer from 0 to 20 GigaHerz, co-authored by Army researchers Drs. David Meyer, Paul Kunz, and Kevin Cox

The researchers plan additional development to improve the signal sensitivity of the Rydberg spectrum analyzer, aiming to outperform existing state-of-the-art technology.

"Significant physics and engineering effort is still necessary before the Rydberg analyzer can integrate into a field-testable device," Cox said. "One of the first steps will be understanding how to retain and improve the device's performance as the sensor size is decreased. The Army has emerged as a leading developer of Rydberg sensors, and we expect more cutting-edge research to result as this futuristic technology concept quickly becomes a reality."

51 IBM and Microsoft close the gap to mainstream quantum computing

by Cliff Saran

https://www.computerweekly.com/news/252495849/IBM-and-Microsoft-close-the-gap-to-mainstream-Quantum-computing

The company has fleshed out its roadmap, originally unveiled in September 2020, to include the software layers required to make quantum computing more accessible to more software developers.

During 2021, IBM said it plans to extend its Qiskit execution environment to increase the capacity to run more circuits at a much faster rate, and adding the capability to store quantum programs so that other users can run them as a service. This could pave the way to making quantum computing available as a service within enterprises.

By 2023, IBM said it plans to offer entire families of pre-built runtimes, callable from a cloud-based application programming interface (API) using a variety of common development frameworks to apply quantum computing to tackle industry-specific problems.

In a blog post describing the roadmap, IBM wrote: "A big part of our software strategy is to continue to use and create open source tools, eventually converting some into first-class cloud-native components. This will allow us to continue scaling and extending our quantum software so that users can take advantage of our architecture while running quantum programs in a secure and reliable way."

"On the other side, users will be able to install and use some components from our software stack directly in their preferred cloud architectures."

IBM is not the only company this week to announce functionality to further the development of mainstream quantum computing. In a Microsoft blog, Krysta Svore, general manager at Microsoft Quantum, unveiled a public preview of the company's cloud-based quantum computing service. "You can access quantum computing capabilities in the cloud from our hardware partners, Honeywell Quantum Solutions and IonQ, through their trapped-ion quantum systems," she wrote.

Those who participate in the public preview will also be able to use "solvers" from Microsoft and 1QBit, said Svore. These are algorithms that apply quantum principles for increased speed and accuracy, running at scale on existing CPU (traditional processors), GPU (graphics processing unit) and FPGA (field programmable gate array)-based hardware.

She added: "With cloud-based access through Azure Quantum, you can accelerate research into solving problems in chemistry, medicine, finance and logistics."

These developments suggest that some organisations may be using cloud-based quantum computing as an integral component of a broad IT architecture within four years. Just as GPUs and FPGAs, particularly when accessed via cloud platforms, have accelerated artificial intelligence training and inference applications, quantum computing promises to solve many of today's insoluble problems.

The developments from companies like IBM and Microsoft illustrate how the industry will deliver quantum computing to the enterprise software market. But a new short film, Quantum ethics, highlights the risks.

The experts featured in the film warn that society needs to think through the implication of what it means to solve problems that were previously insoluble and what regulatory framework needs to be in place to prevent misuse or exploiting quantum computing for malicious intent.

52 New EU Quantum Flagship consortium launches a project on silicon spin qubits as a platform for large-scale quantum computing

https://qutech.nl/2021/02/04/new-eu-quantum-flagship-consortium-launches-a-project-on-silicon-spin-qubits-as-a-platform-for-large-scale-quantum-computing/?cn-reloaded=1

A European consortium was launched today with the goal of scaling silicon quantum technologies. Named QLSI (Quantum Large-Scale Integration with Silicon), this four-year EU project, coordinated by CEA-Leti, will lay the foundation for the EU's industrial-scale implementation of semiconductor quantum processors and position Europe as a global leader in quantum computing. The project will focus on demonstrating that spin qubits are the leading platform for scaling to very large numbers of quantum bits, or qubits, the

building blocks of quantum information processing.

The QLSI consortium features a dynamic team with a complementary skillset, bringing together experienced academics with deep knowledge of in silicon nanostructures and spin qubits, RTOs with silicon CMOS technology expertise, major international businesses in the semiconductor and computing industries, as well as Europe's thriving quantum start-up sector. Each member brings state-of-the-art expertise in their area required to address the challenges of building a scalable quantum computer.

The partners have already realized many of the key advances in the field of silicon quantum. For instance, QuTech, a collaboration between TU Delft and TNO, implemented quantum algorithms in this platform and offers the first online open access quantum computer hosting a 2-qubit quantum chip based on silicon spins through Quantum Inspire. The QLSI consortium will take this principle to the next level with the demonstration of a 16-qubit chip, and will also make an 8-qubit chip available for external use through the Quantum Inspire open-access quantum cloud environment. What makes silicon so attractive? Owing to their experience, the partners have already quantified promising single qubit performance: small size, high fidelity, fast read-out and manipulation. Working with silicon, the next step is to leverage the vast infrastructure of the global semiconductor industry.

Superposition and entanglement

While classical computers use information as bits that are either off or on, represented by '0' or '1', quantum systems utilize superposition and entanglement of particles, such as electrons or photons, or other quanta. In superposition, these qubits are at 0 and 1 states simultaneously. When qubits get entangled, a primary feature of quantum mechanics, a change in one of them causes the other to also change.

Harnessing these features will make it possible to use quantum effects to make major advances in computing, sensing and metrology, simulations, cryptography, and telecommunications. Society's benefits from quantum computing ultimately will include ultra-precise sensors for use in medicine, quantum-based communications, and hacking-proof digital data. In the long term, quantum computing has the potential to solve computational problems that would take current supercomputers longer than the age of the universe. These systems will also be able to recognize patterns and train artificial intelligence systems.

High-stakes, global competition

"Europe is well-positioned to take the EU's spin-qubit R&D to the next level, in what is a high-stakes competition among advanced technological countries," said Maud Vinet, CEA-Leti's quantum hardware program manager, who will lead the four-year, €15 million ($17.7 million) project. "The QLSI project ramps up a dedicated effort across all leading European groups in the field of spin qubits to develop complete processor systems that eventually will reach the thousands of qubits expected as a first step to show the potential for universal, error-corrected quantum computing."

Within the QLSI project QuTech will upgrade Quantum Inspire to include an 8-qubit spin quantum chip to demonstrate a high-quality quantum processor in a semi-industrial environment.

QLSI will pursue four essential results:

- Fabrication and operation of 16-qubit quantum processors based on industry-compatible semiconductor technology

- Demonstration of high-fidelity (¿99%) single- and two-qubit gates, read-out and initialization with these devices in a lab environment
- Demonstration of a quantum computer prototype, with online open-access for the community, integrating such a high-quality quantum processor in a semi-industrial environment (up to eight qubits available online), and
- Documentation of the requirements to address important issue of scalability towards large systems ¿1,000 qubits.

The project is a recent addition to the EU's ambitious Quantum Flagship program, a 10-year, €1 billion ($1.18 billion) R&D initiative launched in 2018. It is a coherent set of research and innovation projects selected through a thorough peer-review process. The overall goal is to consolidate and expand European scientific leadership and excellence in quantum computing, to kick-start a competitive European industry in quantum technologies and to make Europe a dynamic and attractive region for innovative research, business and investments in this field.

19 QLSI members for a consortium fully dedicated to quantum hardware solution delivery

- CEA – development and fabrication of spin qubits
- TU Delft/QuTech – materials development and multi-qubit control
- CNRS – demonstration of spin qubits
- IMEC – significant technological developments aiming at spin qubits
- TNO/QuTech – Spin qubit full stack demonstrator
- Fraunhofer institutes IPMS & IAF – significant technological developments aiming at spin qubits
- of Copenhagen – demonstration and characterization of spin qubits
- UCL – physics experience and charge-and-spin properties of Si nanostructures
- FORSCHUNGSZENTRUM JULICH / FZJ – demonstration of spin qubits
- of Basel – physics experience and charge-and-spin properties of Si nanostructures
- of Twente – physics experience and charge-and-spin properties of Si nanostructures
- Hitachi – physics experience and charge-and-spin properties of Si nanostructures
- of Konstanz – theoretical simulations and modelling of spin qubits and their properties
- IHP (Leibniz-Institut) – development of Si-based quantum materials for spin qubits
- ATOS – development of quantum validation platform
- STMicrolectronics – development of quantum validation platform
- Infineon Dresden – development and fabrication of spin qubits
- Quantum Motion – design and validation of spin qubit devices and architectures
- Soitec – significant technological developments aiming at spin qubits

53 IBM quantum computers now finish some tasks in hours, not months

by J. Fingas

https://www.engadget.com/ibm-quantum-computing-speedup-050134678.html

As much as quantum computers have improved, they're far from taking the reins from conventional computers in some situations. IBM might have made them more practical, however. The tech pioneer has found a way to combine a new program execution environment, Qiskit, with a balance of "classical" and quantum computing to deliver a 100 times speedup for tasks that depend on iterative circuit execution. Computations that take months now will take mere hours, IBM said.

Qiskit by itself allows more circuits to run at a "much faster" rate, and can store quantum programs so that other users can run them. However, it also uploads programs to conventional hardware sitting next to the quantum machines. Before you ask, this isn't really cheating – the move is meant to cut the latency between a user's computer and the quantum chip.

IBM expects to release Qiskit sometime in 2021. Its roadmap also has quantum systems handling a wider range of circuits, and thus a wider range of computing challenges, by 2022. New control systems and libraries in 2023 will help IBM reach its goal of running systems with 1,000 or more qubits, taking the company closer to a "quantum advantage" where the technology can handle at least some tasks more efficiently or cost-effectively than traditional hardware.

The company was quick to acknowledge that there's a long road ahead. It likened current quantum technology to the earliest computers – that is, they required a lot of manual programming and took ages to complete workloads that now seem trivial. Ideally, Qiskit and improved hardware will lead to a day when anyone can put quantum computing to use, even if it's through a distant mainframe.

03 Feb 2021

54 Google says it's too easy for hackers to find new security flaws

by Patrick Howell O'Neillarchive

https://www.technologyreview.com/2021/02/03/1017242/google-project-zero-day-flaw-security/

In December 2018, researchers at Google detected a group of hackers with their sights set on Microsoft's Internet Explorer. Even though new development was shut down two years earlier, it's such a common browser that if you can find a way to hack it, you've got a potential open door to billions of computers.

The hackers were hunting for, and finding, previously unknown flaws, known as zero-day vulnerabilities.

Soon after they were spotted, the researchers saw one exploit being used in the wild. Microsoft issued a patch and fixed the flaw, sort of. In September 2019, another similar vulnerability was found being exploited by the same hacking group.

More discoveries in November 2019, January 2020, and April 2020 added up to at least five zero-day vulnerabilities being exploited from the same bug class in short order. Microsoft issued multiple security

updates: some failed to actually fix the vulnerability being targeted, while others required only slight changes that required just a line or two to change in the hacker's code to make the exploit work again.

This saga is emblematic of a much bigger problem in cybersecurity, according to new research from Maddie Stone, a security researcher at Google: that it's far too easy for hackers to keep exploiting insidious zero-days because companies are not doing a good job of permanently shutting down flaws and loopholes.

The research by Stone, who is part of a Google security team known as Project Zero, spotlights multiple examples of this in action, including problems that Google itself has had with its popular Chrome browser.

"What we saw cuts across the industry: Incomplete patches are making it easier for attackers to exploit users with zero-days," Stone said on Tuesday at the security conference Enigma. "We're not requiring attackers to come up with all new bug classes, develop brand new exploitation, look at code that has never been researched before. We're allowing the reuse of lots of different vulnerabilities that we previously knew about."

Low hanging fruit

Project Zero operates inside Google as a unique and sometimes controversial team that is dedicated entirely to hunting the enigmatic zero-day flaws. These bugs are coveted by hackers of all stripes, and more highly prized than ever before – not necessarily because they are getting harder to develop, but because, in our hyperconnected world, they're more powerful.

Over its six-year lifespan, Google's team has publicly tracked over 150 major zero-day bugs, and in 2020 Stone's team documented 24 zero-days that were being exploited – a quarter of which were extremely similar to previously disclosed vulnerabilities. Three were incompletely patched, which meant that it took just a few tweaks to the hacker's code for the attack to continue working. Many such attacks, she says, involve basic mistakes and "low hanging fruit."

For hackers, "it's not hard," Stone said. "Once you understand a single one of those bugs, you could then just change a few lines and continue to have working zero-days."

Why aren't they being fixed? Most of the security teams working at software companies have limited time and resources, she suggests – and if their priorities and incentives are flawed, they only check that they've fixed the very specific vulnerability in front of them instead of addressing the bigger problems at the root of many vulnerabilities.

Other researchers confirm that this is a common problem.

"In the worst case, a couple of zero-days that I discovered were an issue of the vendor fixing something on one line of code and, on literally the next line of code, the exact same type of vulnerability was still present and they didn't bother to fix it," says John Simpson, a vulnerability researcher at the cybersecurity firm Trend Micro. "We can all talk till we're blue in the face but if organizations don't have the right structure to do more than fix the precise bug reported to them, you get such a wide range of patch quality."

A big part of changing this comes down to time and money: giving engineers more space to investigate new security vulnerabilities, find the root cause, and fix the deeper issues that often surface in individual vulnerabilities. They can also complete variant analysis, Stone said: looking for the same vulnerability in different places, or other vulnerabilities in the same blocks of code.

Different fruit altogether

Some are already trying different approaches. Apple, for example, has managed to fix some of the iPhone's most serious security risks by rooting out vulnerabilities at a deeper level.

In 2019 another Google Project Zero researcher, Natalie Silvanovich, made headlines when she presented critical zero-click, zero-day bugs in Apple's iMessage. These flaws allowed an attacker to take over a person's entire phone without ever requiring the victim to do anything – even if you didn't click a link, your phone could still be controlled by hackers. (In December 2020, new research found a hacking campaign against journalists exploiting another zero-click zero-day attack against iMessage.)

Instead of narrowly approaching the specific vulnerabilities, the company went into the guts of iMessage to address the fundamental, structural problems that hackers were exploiting. Although Apple never said anything about the specific nature of these changes – it just announced a set of improvements with its iOS 14 software update – Project Zero's Samuel Groß recently closely dissected iOS and iMessage and deduced what had taken place.

The app is now isolated from the rest of the phone with a feature called BlastDoor, written in a language called Swift which makes it harder for hackers from accessing iMessage's memory.

Apple also altered the architecture of iOS so that it's more difficult to access the phone's shared cache – a signature of some of the most high-profile iPhone hacks in recent years.

Finally, Apple blocked hackers from trying "brute force" attacks over and over in rapid succession. New throttling features mean that exploits that might have once taken minutes can now take hours or days to complete, making them much less enticing for hackers.

"It's great to see Apple putting aside the resources for these kinds of large refactorings to improve end users' security," Groß wrote. "These changes also highlight the value of offensive security work: not just single bugs were fixed, but instead structural improvements were made based on insights gained from exploit development work."

The consequences of hacks become greater as we become more and more connected, which means it's more important than ever for tech companies to invest in and prioritize major cybersecurity problems that give birth to entire families of vulnerabilities and exploits.

"A piece of advice to their higher ups is invest, invest, invest," Stone explained. "Give your engineers time to fully investigate the root cause of vulnerabilities and patch that, give them leeway to do variant analysis, reward work in reducing technical debt, focus on systemic fixes."

55 Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency

by Christopher Bing, Jack Stubbs, Raphael Satter, Joseph Menn

https://www.reuters.com/article/us-cyber-solarwinds-china-idUSKBN2A22K8

Suspected Chinese hackers exploited a flaw in software made by SolarWinds Corp to help break into U.S. government computers last year, five people familiar with the matter told Reuters, marking a new twist in a sprawling cybersecurity breach that U.S. lawmakers have labeled a national security emergency.

Two people briefed on the case said FBI investigators recently found that the National Finance Center, a federal payroll agency inside the U.S. Department of Agriculture, was among the affected organizations,

raising fears that data on thousands of government employees may have been compromised.

The software flaw exploited by the suspected Chinese group is separate from the one the United States has accused Russian government operatives of using to compromise up to 18,000 SolarWinds customers, including sensitive federal agencies, by hijacking the company's Orion network monitoring software.

Security researchers have previously said a second group of hackers was abusing SolarWinds' software at the same time as the alleged Russian hack, but the suspected connection to China and ensuing U.S. government breach have not been previously reported.

Reuters was not able to establish how many organizations were compromised by the suspected Chinese operation. The sources, who spoke on condition of anonymity to discuss ongoing investigations, said the attackers used computer infrastructure and hacking tools previously deployed by state-backed Chinese cyberspies.

Two people briefed on the case said FBI investigators recently found that the National Finance Center, a federal payroll agency inside the U.S. Department of Agriculture, was among the affected organizations, raising fears that data on thousands of government employees may have been compromised.

The software flaw exploited by the suspected Chinese group is separate from the one the United States has accused Russian government operatives of using to compromise up to 18,000 SolarWinds customers, including sensitive federal agencies, by hijacking the company's Orion network monitoring software.

Security researchers have previously said a second group of hackers was abusing SolarWinds' software at the same time as the alleged Russian hack, but the suspected connection to China and ensuing U.S. government breach have not been previously reported.

Reuters was not able to establish how many organizations were compromised by the suspected Chinese operation. The sources, who spoke on condition of anonymity to discuss ongoing investigations, said the attackers used computer infrastructure and hacking tools previously deployed by state-backed Chinese cyberspies.

In the case of the sole client it knew about, SolarWinds said the hackers only abused its software once inside the client's network. SolarWinds did not say how the hackers first got in, except to say it was "in a way that was unrelated to SolarWinds."

The FBI declined to comment.

Although the two espionage efforts overlap and both targeted the U.S. government, they were separate and distinctly different operations, according to four people who have investigated the attacks and outside experts who reviewed the code used by both sets of hackers.

While the alleged Russian hackers penetrated deep into SolarWinds network and hid a "back door" in Orion software updates which were then sent to customers, the suspected Chinese group exploited a separate bug in Orion's code to help spread across networks they had already compromised, the sources said.

'EXTREMELY SERIOUS BREACH'

The side-by-side missions show how hackers are focusing on weaknesses in obscure but essential software products that are widely used by major corporations and government agencies.

"Apparently SolarWinds was a high value target for more than one group," said Jen Miller-Osborn, the deputy director of threat intelligence at Palo Alto Networks' Unit42.

Former U.S. chief information security officer Gregory Touhill said separate groups of hackers targeting the same software product was not unusual. “It wouldn’t be the first time we’ve seen a nation-state actor surfing in behind someone else, it’s like drafting’ in NASCAR,” he said, where one racing car gets an advantage by closely following another’s lead.

The connection between the second set of attacks on SolarWinds customers and suspected Chinese hackers was only discovered in recent weeks, according to security analysts investigating alongside the U.S. government.

Reuters could not determine what information the attackers were able to steal from the National Finance Center (NFC) or how deep they burrowed into its systems. But the potential impact could be “massive,” former U.S. government officials told Reuters.

The NFC is responsible for handling the payroll of multiple government agencies, including several involved in national security, such as the FBI, State Department, Homeland Security Department and Treasury Department, the former officials said.

Records held by the NFC include federal employee social security numbers, phone numbers and personal email addresses as well as banking information. On its website, the NFC says it “services more than 160 diverse agencies, providing payroll services to more than 600,000 Federal employees.”

“Depending on what data were compromised, this could be an extremely serious breach of security,” said Tom Warrick, a former senior official at the U.S Department of Homeland Security. “It could allow adversaries to know more about U.S. officials, improving their ability to collect intelligence.”

02 Feb 2021

56 Scientists Achieve ‘Transformational’ Breakthrough in Scaling Quantum Computers

by PETER DOCKRILL

https://www.sciencealert.com/scientists-achieve-transformational-breakthrough-in-scaling-up-quantum-computers

Scientists have developed a new kind of cryogenic computer chip capable of functioning at temperatures so cold, it approaches the theoretical limit of absolute zero.

This cryogenic system, called Gooseberry, lays the groundwork for what could be a revolution in quantum computing – enabling a new generation of machines to perform calculations with thousands of qubits or more, whereas today’s most advanced devices comprise only dozens.

“The world’s biggest quantum computers currently operate with just 50 or so qubits,” explains quantum physicist David Reilly from the University of Sydney and Microsoft’s Quantum Laboratory.

“This small scale is partly because of limits to the physical architecture that control the qubits.”

That physical architecture is constrained because of the extreme conditions qubits need to perform quantum mechanical calculations.

Unlike the binary bits in traditional computers, which take either a 0 or 1 value, qubits occupy what is known as the quantum superposition - an undefined and unmeasured state that can effectively represent both 0 and 1 at the same time in the context of a larger mathematical operation.

This esoteric principle of quantum mechanics means quantum computers can theoretically solve vastly complex mathematical problems that classic computers would never be able to answer (or take years trying).

Like with conventional technology, though, more is always better, and to date, researchers have been limited in how many qubits they've been able to successfully deploy into quantum systems.

One of the reasons for that is qubits need extreme levels of cold to function (in addition to other controlled conditions), and the electrical wiring used in today's quantum computer systems inevitably output small but sufficient levels of heat that disrupt the thermal requirements.

Scientists are looking into ways to get around that, but many quantum innovations to date have depended on contriving bulky wiring rigs to keep temperatures stable for increasing qubit counts, but that solution has its own limits.

"Current machines create a beautiful array of wires to control the signals; they look like an inverted gilded birds' nest or chandelier," Reilly says.

"They're pretty, but fundamentally impractical. It means we can't scale the machines up to perform useful calculations. There is a real input-output bottleneck."

The solution to that bottleneck could be Gooseberry: a cryogenic control chip that can operate at 'millikelvin' temperatures just a tiny fraction of a degree above absolute zero, as described in a new study.

That extreme thermal capacity means it can sit inside the super-cold refrigerated environment with the qubits, interfacing with them and passing signals from the qubits to a secondary core that sits outside in another extremely cold tank, immersed in liquid helium.

In doing so, it removes all the excess wiring and the surplus heat they generate, meaning contemporary qubit bottlenecks in quantum computing could soon be a thing of the past.

"The chip is the most complex electronic system to operate at this temperature," Reilly explained to Digital Trends.

"This is the first time a mixed-signal chip with 100,000 transistors has operated at 0.1 kelvin, [the equivalent to] -459.49-degrees Fahrenheit, or -273.05-degrees Celsius."

Ultimately, the team expects their system could enable thousands of qubits to be controlled by the cryogenic chip – roughly a 20-fold increase in what's possible today. In the future, the same sort of approach might enable quantum computers on a whole other level.

"Why not start thinking about billions of qubits?" Reilly told the Australian Financial Review. "The more qubits we can control, the better."

While it may be some time before we see this cryogenic breakthrough put to practical use outside the lab, there's no doubting we're looking at a big step forward in quantum computing, experts say.

"This is going to be transformational in the next few years," Andrew White, the director of the ARC Centre of Excellence for Engineered Quantum Systems, who wasn't involved with the study but oversees quantum research in Australia, told ABC News.

"If everyone [developing quantum computers] isn't using this chip, they will be using something inspired by it."

57 NIST Offers Tools to Help Defend Against State-Sponsored Hackers

by Chad Boutin

https://www.nist.gov/news-events/news/2021/02/nist-offers-tools-help-defend-against-state-sponsored-hackers

Nations around the world are adding cyberwarfare to their arsenal, employing highly skilled teams to launch attacks against other countries. These adversaries are also called the "advanced persistent threat," or APT, because they possess the tools and resources to pursue their objectives repeatedly over an extended period, adapting to defenders' efforts to resist them.

Vulnerable data includes the sensitive but unclassified information managed by government, industry and academia in support of various federal programs. Now, a finalized publication from the National Institute of Standards and Technology (NIST) provides guidance to protect such "controlled unclassified information" (CUI) from the APT. NIST's Special Publication (SP) 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST SP 800-171, offers a set of tools designed to counter the efforts of state-sponsored hackers and complements another NIST publication aimed at protecting CUI.

"Cyberattacks are conducted with silent weapons, and in some situations those weapons are undetectable," said Ron Ross, a computer scientist and a NIST fellow. "Because you may not 'feel' the direct effects of the next hack yet, you may think it is coming someday down the road; but in reality, it's happening right now."

The federal government relies heavily on nonfederal service providers to help carry out a wide range of missions using information systems – a term that includes computers, but also a range of other specialized technologies such as industrial control systems and the Internet of Things. The protection of sensitive federal information that resides in nonfederal systems – such as those used by state and local governments, colleges and universities, and independent research organizations – is of paramount importance, as it can directly impact the federal government's ability to carry out its operations. A hack in 2018 that compromised sensitive information directly inspired the NIST team's work on SP 800-172.

Formerly numbered SP 800-171B during its draft stages, SP 800-172 offers additional recommendations for handling CUI in situations where that information runs a higher than usual risk of exposure. CUI includes a wide variety of information types, from individuals' names or Social Security numbers to critical defense information.

"We developed SP 800-171 in response to major cyberattacks on U.S. critical infrastructure, and its companion document SP 800-172 is designed to mitigate attacks from advanced cyber threats such as the APT," Ross said. "Implementing the cyber safeguards in SP 800-172 will help system owners protect what state-level hackers have considered to be particularly high-value targets: sensitive information about people, technologies, innovation and intellectual property, the revelation of which could compromise our economy and national security."

The enhanced security requirements are to be implemented in addition to those in SP 800-171, since that publication is not designed to address the APT. The requirements in SP 800-172 apply to the components of nonfederal systems that process, store or transmit CUI or that provide protection for such components. To further narrow the scope, the requirements are applied only when the designated CUI is associated with a critical program or high-value asset – the highest priority for protection.

Developed primarily for administrators such as program managers, CIOs and system auditors, the

publication addresses the protection of CUI for system components by promoting penetration-resistant architecture, damage-limiting operations, and designs to achieve cyber resiliency and survivability. Its tools, divided into 14 families, are not intended to be implemented en masse, but selected according to the needs of the organization.

"Most likely an organization implementing this guidance will not want to use all of the enhanced security requirements we offer here," Ross said. "The decision to select a particular set of enhanced security requirements will be based on your mission and business needs – and then guided and informed by ongoing risk assessments."

In response to feedback received during the public comment period, the final draft includes updated scoping and applicability guidance and a more flexible requirements selection approach to allow organizations to customize their security solutions.

Ross said that the tools in the new publication should offer hope to anyone seeking to defend against hacks, even by as intimidating a threat as the APT.

"The adversaries are bringing their 'A-game' in these cyberattacks 24 hours a day, 7 days a week," he said. "You can start making sure the damage is minimized if you use SP 800-172's cyber safeguards."

58 Beyond qubits: Next big step to scale up quantum computing

by Plato

https://zephyrnet.com/beyond-qubits-next-big-step-to-scale-up-quantum-computing/

Scientists and engineers at the University of Sydney and Microsoft Corporation have opened the next chapter in quantum technology with the invention of a single chip that can generate control signals for thousands of qubits, the building blocks of quantum computers.

"To realise the potential of quantum computing, machines will need to operate thousands if not millions of qubits," said Professor David Reilly, a designer of the chip who holds a joint position with Microsoft and the University of Sydney.

"The world's biggest quantum computers currently operate with just 50 or so qubits," he said. "This small scale is partly because of limits to the physical architecture that control the qubits."

"Our new chip puts an end to those limits."

The results have been published in Nature Electronics.

Most quantum systems require quantum bits, or qubits, to operate at temperatures close to absolute zero (-273.15 degrees). This is to prevent them losing their 'quantumness', the character of matter or light that quantum computers need to perform their specialised computations.

In order for quantum devices to do anything useful, they need instructions. That means sending and receiving electronic signals to and from the qubits. With current quantum architecture, that involves a lot of wires.

"Current machines create a beautiful array of wires to control the signals; they look like an inverted gilded birds' nest or chandelier. They're pretty, but fundamentally impractical. It means we can't scale the machines up to perform useful calculations. There is a real input-output bottleneck," said Professor Reilly, also a Chief Investigator at the ARC Centre for Engineered Quantum Systems (EQUS) .

Microsoft Senior Hardware Engineer, Dr Kushal Das, a joint inventor of the chip, said: "Our device does away with all those cables. With just two wires carrying information as input, it can generate control signals for thousands of qubits.

"This changes everything for quantum computing."

The control chip was developed at the Microsoft Quantum Laboratories at the University of Sydney, a unique industry-academic partnership that is changing the way scientists tackle engineering challenges.

"Building a quantum computer is perhaps the most challenging engineering task of the 21st century. This can't be achieved working with a small team in a university laboratory in a single country but needs the scale afforded by a global tech giant like Microsoft," Professor Reilly said.

"Through our partnership with Microsoft, we haven't just suggested a theoretical architecture to overcome the input-output bottleneck, we've built it.

"We have demonstrated this by designing a custom silicon chip and coupling it to a quantum system," he said. "I'm confident to say this is the most advanced integrated circuit ever built to operate at deep cryogenic temperatures."

If realised, quantum computers promise to revolutionise information technology by solving problems beyond the scope of classical computers in fields as diverse as cryptography, medicine, finance, artificial intelligence and logistics.

01 Feb 2021

59 Chinese researchers to send an 'uncrackable' quantum message to space

by Rafi Letzter

https://www.livescience.com/super-secure-quantum-messages-headed-to-space.html

Uncrackable quantum messages can now be sent through the air and will soon be beamed into space.

Researchers at the University of Science and Technology in China (USTC) worked out in 2018 how to secretly share "quantum keys" between orbiting satellites and ground stations, as Live Science previously reported. That made the connection between the Chinese Micius satellite and three ground sites it communicates with in Europe and Asia by far the largest secure quantum network in the world. But the quantum secrecy tool Micius originally used had a few leaks, requiring scientists to develop a more advanced form of quantum encryption known as measurement-device-independent quantum key distribution (MDI-QKD). Now, those same researchers have, for the first time, pulled off MDI-QKD wirelessly, across a city in China, without any fiber optics involved. And they're getting ready to send MDI-QKD up to Micius.

"The results by the Chinese group [are] very interesting for the quantum communication community," said Daniel Oblak, a quantum communications researcher at the University of Calgary in Ontario who did not work on the experiment.

It opens the door, he said, to practical quantum-encrypted networks relying on both satellites and fiber-optic cables working in tandem, something not possible with current technology.

Quantum-secure messages

Every bit of secure data you've ever sent from your phone – instructions to your bank through a mobile app, for example, or Whatsapp messages with your mom – has been broadcast across huge distances full of potential hackers. But any snoops listening in probably couldn't make any sense of that information because it was transformed into gibberish that could only be deciphered with a secure key, basically a long string of numbers. That string of numbers gets scrambled up with the information it protects, and only someone who knows the string can unscramble them.

Those systems aren't perfect though, vulnerable to attack from anyone who listened in when the key was being shared. They also don't typically use sufficiently long strings of numbers to be perfectly secure even against someone who didn't listen in on the key, according to Belgian cryptographer Gilles Van Assche's book "Quantum Cryptography and Secret-Key Distillation".

So in the 1980s, researchers developed a theoretical method for generating secure keys using quantum mechanics. They figured out that secure keys could be encoded into the quantum properties of individual particles, and exchanged secretly back and forth. The advantage of this "quantum key distribution" (QKD) is that quantum physics dictates that the very act of observing a particle irreparably changes it. So any spies who tried to intercept the quantum key could be immediately detected by the changes in the particles.

Get ready to explore the wonders of our incredible universe! The "Space.com Collection" is packed with amazing astronomy, incredible discoveries and the latest missions from space agencies around the world. From distant galaxies to the planets, moons and asteroids of our own solar system, you'll discover a wealth of facts about the cosmos, and learn about the new technologies, telescopes and rockets in development that will reveal even more of its secrets.

Securing the quantum vault

In recent years, as researchers began building prototype quantum key distribution networks using photons (light particles), an important flaw turned up in the system – "Side channel attacks" could siphon copies of a quantum key directly from the receiver, a study published in 2012 in the journal Physical Review Letters found.

So researchers developed MDI-QKD, calling it in that 2012 paper "a simple solution to remove all (existing and yet to be discovered) detector side channels."

In MDI-QKD, both the sender and receiver of a message send their quantum key photons at the same time (as well as decoys) to a third party. Each photon contains a single bit of information: a one or a zero. The third party doesn't have to be secure, and it can't read the information the photons convey.

"All it can tell is the relation between the [photons]," said Wolfgang Tittel, a quantum communications expert with QuTech, a collaboration between Delft University of Technology in the Netherlands and the Netherlands Organization for Applied Scientific Research. It can just say "whether they are the same or different."

When both the sender and the receiver send a one or a zero, they get a message from the relay saying they sent the same bit. If they send different numbers, the relay broadcasts that they sent different numbers. A hacker spying on the relay could only tell whether the photons were the same or different, but not whether they represented a one or a zero.

"But of course the people who sent the states know what they sent, so they know what the other person sent," Tittel told Live Science.

All those ones and zeros add up to a secure quantum key, and there's no way for a hacker to tell what

it is.

But MDI-QKD has its own challenges, said Tittel, who was not involved with this latest experiment. It requires that both photons arrive at the relay at precisely the same time.

"We found that this is difficult because of changes in the temperature of the device," he said, which can mess up the timing.

And that's using dedicated fiber-optic cables. Sending photons through the air requires accounting for atmospheric turbulence, which makes timing even more unpredictable.

That's why the new experiment is so impressive, Tittel said. While China has been doing standard QKD with Micius since 2018, no one had until now figured out how to do the more unbreakable encryption system over long distances without fiber-optic cables to carry the photons back and forth.

In the new study, the researchers sent a MDI-QKD secure key across 11.9 miles (19.2 kilometers) of open air between two buildings in the city of Hefei. To make sure the photons arrived at the relay at exactly the same time, they developed algorithms that enabled the sender and receiver devices to account for the fluctuations in that stretch of atmosphere.

Getting MDI-QKD into space will require more problem-solving, including better algorithms that can account for the even greater distances involved.

"The second challenge we hope to overcome is associated with the motion of satellites," Qiang Zhang, one of the authors of the paper, told Phys.org.

A moving target changes the behavior of photons in ways that have to be very precisely accounted for in order to make sense of the signal.

Tittel said that the motion of the satellite makes MDI-QKD "very difficult," but that it's plausible the USTC team might pull it off.

If they do, they will have developed a quantum network uncrackable by any known method of codebreaking. It would be the most secure long-distance communication network in the world.

60 Unlocking Innovation in Quantum Computing

by Oxford Instruments NanoScience

https://physicsworld.com/a/think-modular-think-flexible-unlocking-innovation-in-quantum-computing/

If January turns out to be a template for the rest of 2021, the product development team at Oxford Instruments NanoScience is set for a busy year after registering the first industry and academic installations of Proteox, a next-generation dilution refrigerator designed for applications in quantum computing R&D and ultra-low-temperature condensed-matter physics. The customers: Oxford Quantum Circuits (OQC), a University of Oxford start-up that's pioneering a "**quantum computing as a service**" (QCaaS) business model, and the University of Glasgow's quantum circuits group, a multidisciplinary research team working at the frontiers of quantum science, technology and application.

In terms of the back-story, Oxford Instruments NanoScience is a division of parent group Oxford Instruments, a diversified and long-established UK provider of specialist technologies and services to research and industry. The NanoScience business unit, for its part, designs and manufactures research tools to support the development, scale-up and commercialization of next-generation quantum

technologies. Think cryogenic systems (operating at temperatures as low as 5 mK) and high-performance magnets that enable researchers to harness the exotic properties of quantum mechanics – entanglement, tunnelling, superposition and the like – to yield practical applications in quantum computing, quantum communications, quantum metrology and quantum imaging.

Flexible solutions for cold science

It's with this quantum opportunity front-and-centre that the fundamentals of the Proteox dilution refrigerator have been reimagined to support multiple scientific users and a variety of ultra-low-temperature experiments from a single system operating in the mK regime. That scalability is achieved with a side-loading "secondary insert" module that allows samples, communications wiring and signal-conditioning components – basically full experimental set-ups – to be installed and changed whenever necessary.

"Proteox is the largest dilution refrigerator in its class with an extensive capacity for integrating components, experimental services and sample mounting," explains Harriet van der Vliet, product segment manager for quantum technologies at Oxford Instruments NanoScience. "Modularity and flexibility are key," she adds, "and we work closely with our customers to offer them tailored solutions and experimental set-ups on standard lead times."

With adaptability comes future-proofing – effectively a "pay-as-you-grow" offering that allows end-users to add new functionality to Proteox as their research requirements evolve and their funding permits. "The customer can specify an entry-level system that's just a base refrigerator – for example, no magnet and no fast sample exchange," notes van der Vliet. "Over time, as new research grants or start-up investments are secured, it's possible to upgrade your Proteox and purchase different secondary inserts, such as the rapid-sample-exchange bottom-loader, as well as taller frames and a variety of magnets. The freedom to upgrade the Proteox is a key design feature, bringing unparalleled value-for-money to the dry dilution-refrigerator market."

Quantum collaboration

The development of Proteox looks to be well-timed, tapping as it does the growing technology push and commercial pull within the "quantum economy" – not least in the UK. Last year, for example, a research/industry consortium led by OQC, and including Oxford Instruments NanoScience, secured £7 million in funding from Innovate UK, the UK's innovation agency, to fast-track the commercialization of superconducting quantum technologies.

Broadly, that upfront investment will support fabrication of superconducting quantum circuits and the scale-up of core enabling infrastructure such as specialist cryogenic equipment and state-of-the-art test electronics – all of which currently represent a significant barrier to entry for companies seeking to access emerging quantum markets and applications. The consortium is eyeing multiple revenue opportunities in the near term, including QCaaS, cryogenic measurement as a service (MaaS) as well as a contract foundry offering.

Our strategy at OQC is to build the core, in terms of our quantum computer, and to partner with the best," says Ilana Wisby, CEO of OQC. As such, Oxford Instruments NanoScience represents a natural partner when it comes to the enabling cryogenic technologies for QCaaS. "Put simply," adds Wisby, "the Proteox platform allows us to efficiently and reliably generate the ultra-low temperatures needed to operate our quantum computer."

There's a pleasing circularity to this tie-up. While Oxford Instruments was one of the first spin-out companies to emerge from the University of Oxford's research programme (back in 1959), the established manufacturer is now supporting OQC and other start-ups and research groups in the UK's nascent quantum supply chain. That sense of collective endeavour, it seems, also informs OQC's mindset. "With our main focus on QCaaS," notes Wisby, "we do think it's important to play our part in developing a healthy quantum ecosystem for the UK. That will pay off for us in the long run through new collaborations and the opportunity to work with the brightest talents in the field."

Cool customers

The original version of OQC's quantum computer was developed using Triton, the previous generation of cryogen-free refrigeration technology from Oxford Instruments NanoScience. The move to Proteox, and the incorporation of the new refrigeration system into OQC's state-of-the-art laboratory earlier this month, marks a significant milestone in the start-up's commercial roll-out of its QCaaS and MaaS offering. "We've been able to collaborate closely with the engineering team at Oxford Instruments NanoScience to develop high-density wiring solutions that meet our specific requirements," explains Wisby. "Ultimately that is going to help us to scale the number of qubits in a cost- and space-efficient way."

Another feature of Proteox is ease-of-use. For starters, an all-new web-based control system combines remote connectivity with push-button automation routines, while enhanced data interrogation and visualization software offers live plotting of key process parameters – for example, the temperatures and pressures at relevant stages of the system cool-down. "The intuitive user interface ensures we spend our time building cutting-edge quantum computers rather than focusing on whether things get cold," adds Wisby.

61 Azure Quantum is now in Public Preview

by Krysta Svore

https://cloudblogs.microsoft.com/quantum/2021/02/01/azure-quantum-preview/

Azure Quantum, the world's first full-stack, public cloud ecosystem for quantum solutions, is now open for business. Developers, researchers, systems integrators, and customers can use it to learn and build solutions based on the latest innovations – using familiar tools in the most trusted public cloud.

The unified Azure Quantum ecosystem will accelerate your R&D with access to diverse quantum software and hardware solutions, a network of leading quantum researchers and developers, a robust resource library, and flexible self-service or tailored development programs for customers and systems integrators.

Collaborate with a vibrant community of innovators and developers

You'll be able to collaborate with world-leading experts in our vibrant community of quantum innovators. Our open-source Quantum Development Kit (QDK) with the Q# quantum programming language protects your development investments by proactively anticipating and integrating with advances in quantum systems. And Microsoft's new Quantum Intermediate Representation (QIR) is a common open-source interface between languages and target quantum computation platforms.

Wherever you are starting, you can tap into our robust resource library of learning materials and samples to grow your skills in quantum computing and optimization. Microsoft Learn teaches fundamental quantum concepts, Katas teach quantum programming in self-paced tutorials, and our samples demonstrate how quantum algorithms can be used for a variety of quantum computing tasks.

Access quantum computing and optimization solutions in the cloud

Through a single development interface, you can tap into unique capabilities offered by industry leaders in quantum computing and optimization solutions.

You can access quantum computing capabilities in the cloud from our hardware partners, Honeywell Quantum Solutions and IonQ, through their trapped-ion quantum systems. Honeywell's system leverages mid-compute measurement and qubit reuse, allowing developers to write quantum algorithms in uniquely impactful ways. IonQ's system offers a dynamically reconfigurable system for up to 11 fully-connected qubits that lets you run a two-qubit gate between any pair.

You can also drive impact today by developing optimization solutions based on solvers from Microsoft and 1QBit. This new generation of algorithms apply quantum principles for increased speed and accuracy, running at scale on a range of silicon including CPU, GPU and FPGA. With cloud-based access through Azure Quantum, you can accelerate research into solving problems in chemistry, medicine, finance, and logistics.

Explore at your own pace on a trusted, scalable, and secure platform

As you start on your quantum journey, you can explore at your own pace, with the peace of mind that your data is secure in the most-trusted public cloud. You pay as you go, and scale when you are ready. You have the flexibility to choose from self-service development or tailored development services with our Enterprise Acceleration Program.

Attend our free Azure Quantum Developer Workshop on February 2 at 8am PST, when you can learn from our industry-leading partners about the latest in quantum computing and optimization solutions. They will share the capabilities they are delivering along with technical demos and a live Q&A at the end of the workshop.

The transition to Public Preview of Azure Quantum is a key milestone for quantum computing and our ecosystem. This continues the momentum we saw last year, which includes selection for the National Quantum Initiative Quantum Research Centers, the addition of new Azure Quantum partners, and hardware advances in scaling control circuitry for qubits.

Customers using Azure Quantum have already demonstrated valuable ways to build solutions to complex problems. From logistics and freight optimization to risk management solutions and fighting cancer, we're seeing real-world application of Azure Quantum solutions today, and we are pleased to now expand Azure Quantum to Public Preview.

Try Azure Quantum today for free and join the most comprehensive full-stack ecosystem delivering quantum impact.

62 Quantum Computing Scientists Call for Ethical Guidelines

by Sara Castellanos

https://www.wsj.com/articles/quantum-computing-scientists-call-for-ethical-guidelines-11612155660

A group of quantum computing experts, including scientists and company executives, want to raise ethical concerns about the technology's potential to create new materials for war and accelerate human DNA manipulation.

Six experts are featured in a 13-minute video titled "Quantum Ethics: A Call to Action," which goes live Monday on YouTube and the Quantum Daily, a free online source for quantum computing news.

The goal of the video, which features a former quantum chief at Alphabet Inc.'s Google, is to kick off conversations with other quantum computing industry leaders about the ethical implications of the technology.

"Whenever we have a new computing power, there is potential for benefit of humanity, [but] you can imagine ways that it would also hurt people," said John Martinis, professor of physics at University of California, Santa Barbara, and former chief scientist of quantum hardware at Google.

While quantum computers are still in their early stages, it is important to begin discussing the potential benefits and drawbacks of the technology and find a way to balance the two, he said. "You want to think ahead," he said.

Dr. Martinis and others such as Ilana Wisby, chief executive of quantum computing company Oxford Quantum Circuits, and Nick Farina, founder and chief executive of quantum computing hardware company EeroQ Corp., are also featured in the short video.

Quantum computers have the potential to dramatically speed up drug and materials discovery as well as complex calculations related to finance. Companies such as Visa Inc. and JPMorgan Chase & Co., Roche Holding AG and Volkswagen AG are all experimenting with early-stage quantum technology.

By harnessing quantum physics, quantum computers have the potential to sort through a vast number of possibilities in nearly real time and come up with a probable solution. While traditional computers store information as either zeros or ones, quantum computers use quantum bits, or qubits, which represent and store information as both zeros and ones simultaneously.

A commercial-grade quantum computer hasn't been built yet, but startups and tech giants including Google, Microsoft Corp. and International Business Machines Corp. are racing to commercialize the technology.

"This is the equivalent of a whole new industrial revolution," said llyas Khan, founder and chief executive of Cambridge Quantum Computing, which develops cybersecurity products, software and algorithms that companies can use when experimenting on early-stage quantum computers. That power, in the wrong hands, could also be used to create harmful materials or to manipulate the human genome in a harmful way, he said. "We ought to have those conversations today," said Mr. Khan, who was also featured in the video.

Though it will likely take years to come up with ethical guidelines for quantum computers, Mr. Khan said he is beginning to speak with government officials in the U.K. about those ethical issues now. There may have been certain ethical controls on technologies such as social media and data privacy if conversations about ethics were had in the mid-1990s, he said. "We were asleep at the wheel," said Mr. Khan.

Experts are already bracing themselves for some of quantum computing's potential challenges. For example, financial services companies are preparing for a time when a powerful quantum computer could break some of the most widespread cryptographic methods currently used in cybersecurity. Hundreds of

the world's top cryptographers are involved in a competition to develop new encryption standards for the U.S. that would guard against both classical and quantum-computing cyberattacks.

Matt Swayne, an editor at the Quantum Daily who co-produced the short video along with Publisher and co-founder Evan Kubes, said he aims to create an advisory group of experts to discuss the topic of quantum ethics. The video is the first step, he said. "We want to raise concern but we don't want to cause fear," he said.

63 Quantum-resistant cryptography technology applied to medical information system

by Lim Chang-won

https://www.ajudaily.com/view/20210201111358948

Quantum-resistant cryptography technology has been applied to a medical information system at a general hospital to strengthen security in a project led by **LG Uplus**, a mobile carrier in South Korea.

LG Uplus (LGU+) has commercialized post-quantum cryptography (PQC) technology, which refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer. Cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat.

LGU+ said on February 1 that it has teamed up with ICTK Holdings, a transaction and security solution provider, to develop an application that utilizes quantum-resistant cryptography for data transmission and reading of a medical information system Eulji Medical Center. The application proved that quantum-resistant cryptography can be used to protect crucial information in medical fields.

Medical personnel can gain access through the process of authenticating servers and public keys with certificates stored on security chips by connecting USB-type security tokens to personal computers and entering IDs and passwords. "We will establish strong security that is valid in the era of quantum computing in all areas where data is delivered to customers as well as telecommunication networks," said Koo Sung-chul, in charge of LGU+'s wired network business.

In December 2020, LGU+ tested the usefulness of PQC technology by applying it to exclusive commercial lines. Data encoded in a quantum state is virtually unhackable without quantum keys which are basically random number tables used to decipher encrypted information.

64 Home working increases cyber-security fears

by David Silverberg and Will Smale

https://www.bbc.com/news/business-55824139

"We see tens of different hacking attacks every single week. It is never ending."

A senior computer network manager for a global financial services company, Peter (who did not want to give his surname, or the name of his employer, due to his firm's anxieties surrounding cyber-security), says they are bombarded from all directions.

"We see everything," he says. "Staff get emails sent to them pretending to be from the service desk, asking them to reset their log-in passwords.

"We see workers being tricked into downloading viruses from hackers demanding ransoms, and we have even had employees sent WhatsApp messages pretending to be from the CEO, asking for money transfers.

"And having staff working from home during the lockdowns has just made it worse, as it is much harder to keep an eye on everyone."

With one in three UK workers currently based exclusively at home, and the same level in the US, this remote working on a vast scale continues to be a major headache for the IT security bosses of companies large and small around the world.

And studies shows that many firms are not taking the issue as seriously as they should. For example, one in five UK home workers has received no training on cyber-security, according to a recent survey by legal firm Hayes Connor Solicitors.

The report also found that two out of three employees who printed potentially sensitive work documents at home admitted to putting the papers in their bins without shredding them first.

Meanwhile, a separate UK study last year found that 57% of IT decision makers believe that remote workers will expose their firm to the risk of a data breach.

"In the rush and panic to set remote working practices up, even simple data protection practices were ignored," says Christine Sabino, a senior associate at Hayes Connor.

"Companies did not provide additional security relating to computers, electronic communication, phone communication."

So what can both companies and home working staff do to make things as safe and secure as possible?

Ted Harrington, a San Diego-based cyber-security specialist, and author of Hackable: How To Do Application Security Right, says firms should have started by giving all home workers a dedicated work laptop. While many larger companies may well have done this, not all smaller firms necessarily have the resources to do so, but Mr Harrington stresses its importance.

"Supply staff with laptops and other equipment that are owned, controlled and configured by the company," he says. "This alleviates the burden on your people to set things up right, and ensures they follow the security controls the company wants."

Definitely don't have staff using their personal computers for work, says Sam Grubb, an Arkansas-based cyber-security consultant, and author of forthcoming book How Cybersecurity Really Works.

"The main problem with using your own computer to do work is that you are not limited in what you can do on it, nor are you necessarily the only one that uses it," he says.

"So while you might not be visiting a shady website to download movies for free, your teenage son could be doing that exact thing on your home laptop without you even knowing.

"This makes it much easier for malware or other attacks to happen. This might affect the work you are doing, or in a worst-case scenario, lead to the compromise of co-workers' devices, or other company devices such as servers."

Mr Harrington says that the next step is that companies must set up a VPN or virtual private network, so that remote computers have secure and encrypted connections with the firm's servers and everyone else in the company.

Mr Grubb uses a transport and wildlife analogy to explain how VPNs work. “A VPN is like a tunnel between two cities,” he says.

“Instead of driving through the dark forest full of tigers, lions and bears, you drive through the underground tunnel, where no one can see you driving until you reach your destination on the other side.”

However, even with work laptops, VPNs and the latest cyber-security software systems in place, staff can still make damaging mistakes, such as falling prey to a “phishing” email – a malicious email pretending to be a legitimate one in order to trick someone into handing over sensitive data.

Currently such scam emails doing the rounds include some that are pretending to be informing the targeted person that they have been exposed to Covid-19, or invited to have the vaccine. They ask the recipient to clink on the link, which then tries to download malware onto his or her computer.

For this reason, both Mr Harrington and Mr Grubb say that it is essential that businesses give staff proper cyber-security training.

“Firms should be providing training to help their employees understand the threats they face,” says Mr Grubb.

Ms Sabino adds that both staff and their bosses need to do their bit. She says, for example, that employees should avoid talking about work on social media, while firms should give shredders to home workers who need to print things out.

With even the most cyber-security aware home workers just one click away from making a mistake, Mr Harrington says that firms need policies in place so that staff know who to immediately report a threat to.

“If an employee falls victim to an attack, make sure that they know a) who to contact, and b) that their outreach is welcome and won’t result in termination,” he says. “You don’t want people afraid of repercussions and thus covering up mistakes.”

Tsedal Neeley, a professor of business administration from Harvard Business School who is an expert on remote working, agrees that home workers should know exactly who to report cyber-security problems to. “Engaging with their firm’s IT/cyber-security experts is crucial,” she says.

Peter, the computer network manager, says this engagement should be frequent. “Users should be suspicious of anything that they are not 100% confident about, and it does not hurt to ask your IT department. It is better to check than be compromised.”