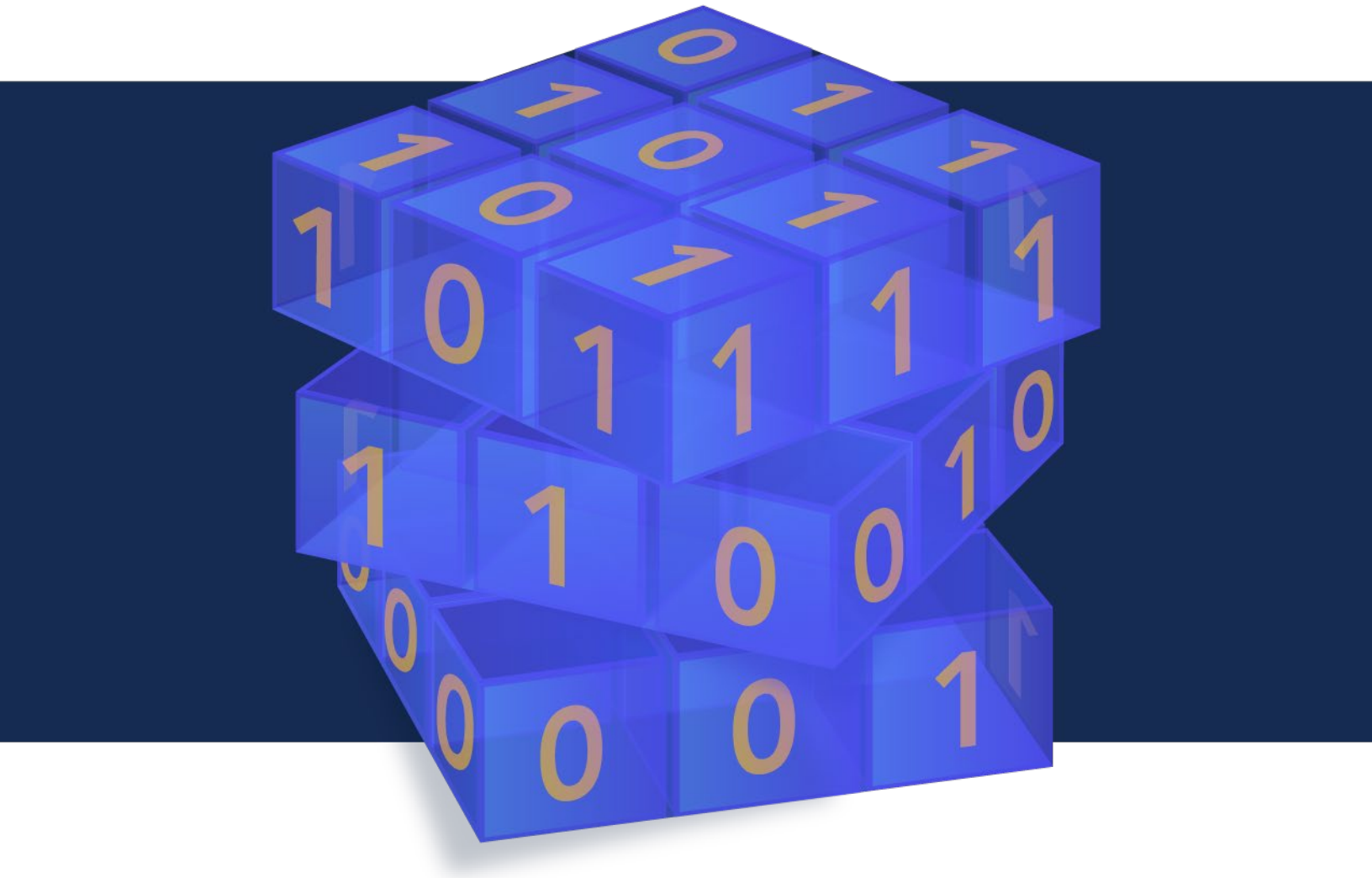
# Crypto News

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

**September 01, 2021**



# Table of Contents



# 1. Editorial

**SEATTLE, WA – September, 1st, 2021**. It's here! The September issue of Crypto News is now ready for you! This month's newsletter includes exciting new findings in quantum computing including when we can expect quantum computers to be right in the palm of our hands in our phones. Check out article 11 which dives into the usability of room temperature qubits made of diamonds! Interested in cryptocurrency? Take a look at article 34 which talks about the potential impact of quantum computers on blockchain security and what can be done to combat the issues. Interested in a career in the up-and-coming Quantum Computing industry? Take a look at article 56 which outlines what types of skills are needed and skills gap currently plaguing the industry. Go ahead … click the link … you won't want to miss the other articles either!

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

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

# 2. EPFL launches new Center for Quantum Science and Engineering

by julien-levallois
https://www.swissquantumhub.com/epfl-launches-new-center-for-quantum-science-and-engineering/

"Developing quantum technology is an incredible venture that puts us face to face with unprecedented scientific and engineering challenges. Meeting these challenges requires a concerted effort from all technical disciplines – physics, mathematics, chemistry, computer science and engineering – more so than for any previous kind of technological development," says Prof. Vincenzo Savona, the head of EPFL'sLaboratory of Theoretical Physics of Nanosystems. "EPFL has a long history of excellence and leadership in these various disciplines and occupies a unique strategic position in quantum science and engineering, both in Switzerland and worldwide."

Prof. Savona, whose expertise spans quantum optics, open quantum systems and quantum information, will be the QSE Center's first director. He will be assisted by a management team composed of professors from EPFL's School of Basic Sciences, School of Engineering and School of Computer and Communication Sciences.

## Major technological advancements

"Thanks to recent progress in science and engineering, we can now use phenomena described by the laws of quantum mechanics to develop revolutionary new technology for computing, communications and measurement," says Prof. Savona. "This will lead to major advancements in several fields and bring significant benefits to society."

By setting up the QSE Center, EPFL aims to coordinate efforts across the board to develop and implement quantum technology in applications that span all disciplines of science and engineering.

What sets the Center apart is its cross-disciplinary approach. Prof. Savona explains: "Quantum technology is highly complex and requires pulling together methods from many scientific fields. The unique feature and key strength of the QSE Center is our ability to bring together experts from different fields – already represented here at EPFL – to apply their knowledge to quantum science and engineering."

## Two main research areas

Research at the QSE Center will focus on two main areas. The first is quantum computing." Our goal here will be to develop and implement quantum algorithms as well as the computer programs needed to use them," says Prof. Savona. "Developing, implementing and integrating these tools will eventually lead to a quantum advantage [see box] in all applications requiring a high level of computing power. These applications could include simulating biological molecules to predict disease and develop new drugs, for example, or running simulations of weather and climate change over extended time horizons. Quantum advantage would also benefit much of the research done here at EPFL, such as in physics, chemistry, materials science, engineering, life science, computer science and data science."

The second research area will involve studying integrated, hybrid and scalable systems using EPFL's advanced nano-fabrication facilities. This will pave the way to technological advancements in quantum hardware, quantum sensing and quantum communications.

## A priority on education and research partnerships

The QSE Center will draw on the wide range of skills in quantum science and engineering already available in Switzerland. For instance, it intends to work closely with the University of Geneva through joint R&D projects and jointly hold classes for Master's and PhD students.

Also with regards to education, the Center will introduce a new Master's program in quantum science and engineering at EPFL. This will be a unique, cross-disciplinary program with classes in theoretical physics, computer science and engineering. "We will also offer excellence fellowships for Master's students in order to attract talented young minds from Switzerland and abroad," says Prof. Savona. "This will enable us to lay the foundation for the next generation of quantum scientists and engineers."

In addition, the QSE Center will promote research and innovation by holding events such as workshops, conferences, and programs on specific topics, bringing selected experts to EPFL for long-term stays. These events will foster interaction and collaboration and stimulate creative thinking and progress.

"Current and future breakthroughs in quantum technology mark major turning points in the history of humanity," says Prof. Savona. "We're in a pioneering era that's similar to the emergence of computers in the 1950s and the advent of the internet in the 1990s. This is a one-of-a-kind opportunity to contribute to the progress and advancement of our society."

# 3. It's not too late for Europe to lead the post-quantum cryptography race

by ANDRÉ LOESEKRUG-PIETRI
https://sifted.eu/articles/europe-post-quantum-cryptography/

The world may be focused on the race to vaccinate — but some necessary sprints should not make us forget about long-term marathons, including post-quantum cryptography (PQC).

A functioning quantum computer will make all current tools for confidential, secure data and communications — also known as cryptography — obsolete. We need new encryption methods that can stand against these new powerful computers. The stakes are high: we also need to master these technologies to avoid having anti-democratic or terrorist groups abuse encryption to act against our open societies.

While the US has taken the lead so far in defining post-quantum cryptography (PQC), Europe also has a chance to become a global leader.

## Europe versus the US

So far, the US has taken the lead in defining PQC. The US's National Institute of Standards and Technology (NIST) started a post-quantum cryptography competition in 2016 to identify cryptographic algorithms able to withstand quantum computer attacks by 2022 — and make them available by 2024. A bit ironic given that five years ago, US entities like the National Security Agency (NSA) were spying on the world.

So how can Europe 'crack the code 'and take a leadership position in PQC? It's actually easier than we might think.

Firstly, we already have the talent here: among the seven NIST finalists, all cryptosystems except one have a majority of European scientists participating in their development. We need to keep those talented individuals in Europe, through less bureaucratic and more purpose-driven funding mechanisms, and through an effective Digital Single Market to build a market on the same scale as the US and China. Otherwise, European policymakers will keep subsidising tech leaders that will then fly over the Atlantic to deploy their solutions.

Secondly, there's a clear window of opportunity for Europe to be the 'third way 'between other tech superpowers, provided they're much more proactive and technologically savvy. In the case of PQC, there are rising concerns over the monopoly that the NIST and the US administration has on the normalization of PQC technology worldwide. The EU can act as the 'kingmaker 'not only in cryptography but also in AI, greentech or healthcare — provided we are bold, fast and agile.

### Defining the code of tomorrow

European policymakers should take note. As the NIST example shows beyond soft and hard power, *regulatory power* can also pave the way for tech dominancy. The NIST (a federal agency of the US Department of Commerce) doesn't have any international legal authority. Yet, since the US hosts by far the biggest postquantum ecosystem, the NIST is in the position to declare standards that will become industry requirements — this already happened in the early 2000s for the standardisation of cryptosystems such as the AES (now the most widely used encryption method in the world) and SHA-3 (now used for some bitcoins).

It's said that 'code is read more than it is written'. In the case of the NIST competition, it highlights on the contrary that policymakers can still define the code of tomorrow — if they act and craft the future now, develop much stronger foresight capabilities and find the missing boldness and agility, by working much more closely with the European technology ecosystem and the civil society.

# 4. IIT Roorkee, IISc Bangalore, C-DAC Develops India's First Quantum Computer Simulator Toolkit

by Bishal Kalita
https://www.ndtv.com/education/iit-roorkee-iisc-bangalore-c-dac-develops-indias-first-quantum-computer-simulator-toolkit

The Ministry of Electronics and Information Technology (MeitY) has launched the country's first 'Quantum Computer Simulator (QSim) Toolkit', brought together by Indian Institute of Science (IISc) Bangalore, Indian Institute of Technology (IIT) Roorkee and Centre for Development of Advanced Computing (C-DAC).

"Quantum Computing is a rapidly emerging computational paradigm which can perform a variety of tasks with greater speed and efficiency than present day digital computers...in areas such as cryptography, computational chemistry and machine learning, quantum computing promises exponential growth in computing power. QSim is a first-of-its-kind toolkit to be indigenously developed and is intended to be a vital tool in learning and understanding the practical aspects of programming...." IIT Roorkee said.

QSim aims to "address the common challenge of advancing the quantum computing research frontiers in India. It will enable researchers and students to research Quantum Computing in a cost-effective manner," it added.

The project was funded by MeitY and developed through a multi-institutional approach by the three institutes.

As part of the "Design and Development of Quantum Computing Toolkit (Simulator, Workbench) and Capacity Building" project, the team from IIT Roorkee helped the teams from IISc, CDAC-Bangalore, CDAC-Hyderabad, in providing the required expertise in quantum computing and developing programs to be tested and implemented on the toolkit.

Shri Rajeev Chandrasekhar, Minister of State, Electronics and IT, said, "This is an important milestone for the Ministry and the entire country towards creating capabilities in strategic areas such as Quantum Computing. It is interesting that we are doing this when we just started celebrating our 75th year of independence.

"This occasion is good to look back on how far we have come as a nation. In many ways QSim and focus on Quantum Computing is about looking ahead to India in another 25 years. I congratulate the team again and all the best to all those involved in this endeavor," the minister said.

Dr Sugata Gangopadhyay, Professor and Head, Department of Computer Science and Engineering, IIT Roorkee, said, "Our team worked closely with the teams from C-DAC on the development of the toolkit. The expertise provided by IIT Roorkee played a significant role in bringing the toolkit to its current state. We are currently working on the development of programs to be implemented on the simulator…."

Prof Ajit K Chaturvedi, Director, IIT Roorkee, said, "IIT Roorkee will continue to play an active role in quantum computing education and research. The quantum simulator being launched today is poised to be a key enabler in this direction."

IIT Roorkee recently introduced two courses in quantum computation. The first course was launched through the E&ICT academy and was attended by over 400 participants.

The second course was offered to scientists and officers at various government agencies and laboratories and was attended by close to 100 participants.

# 5. Arqit and Babcock to Collaborate on Possible Quantum Encryption Use Cases in Government and Defense Market

by Matt Swayne
https://thequantumdaily.com/2021/08/26/arqit-and-babcock-to-collaborate-on-possible-quantum-encryption-use-cases-in-government-and-defense-market/

Arqit Limited, a leader in quantum encryption technology has entered into a collaboration agreement with Babcock International Group, the Aerospace, Defence and security company. The agreement will see the two companies jointly test and experiment with a range of use case scenarios and practical applications for government and defence customers to demonstrate the encryption capabilities of Arqit's QuantumCloud™ product. It will also see Babcock deepen its involvement in important areas of broader Quantum Technology development.

QuantumCloud™ creates software encryption keys, combining patented quantum and classical technologies. The product is simple and efficient to use at any cloud, edge, or end point device with no disruption to hardware or software required. Under the agreement, the software will be tested in live operational scenarios to demonstrate encryption capabilities in a dynamic environment and across a variety of platforms and military networks. This testing will include planned participation in a number of UK Government funded projects.

Specific projects of focus include unmanned ground vehicle programmes, secure manned and unmanned aerial vehicle programmes, secure maritime connectivity programmes and other projects that will come to fruition through ongoing conversations with the UK Government and R&D agencies.

Richard Drake, managing director, Babcock Mission Systems said, "We're continuing to develop our technology strategy with a particular interest in digital technologies, secure communications and other areas such as Artificial Intelligence, Digital Twins and autonomy.

"As threats to data evolve, we need to respond and grow our capabilities in line with new requirements. As such we are delighted to be collaborating with Arqit on this project, broadening our involvement in quantum encryption and enhancing our encryption capability offering to our customers for use on future projects and programmes".

David Williams, Founder of Arqit added, "Partnering with Babcock to apply QuantumCloud™ in live defence use cases is a great opportunity to increase the momentum we have in this market. Following the earlier announcement that QuantumCloud™ 1.0 is now live for commercial customers to use, we are excited to see its use expanding. We are certain that Arqit, uniquely amongst all other companies, has solved the security layer problem in the Joint All Domain Command and Control market. This gives Arqit, a massive near term revenue opportunity"

# 6. Study demonstrates the quantum speed up of supervised machine learning on a new classification task

by Ingrid Fadelli
https://phys.org/news/2021-08-quantum-machine-classification-task.amp#amp_tf=From%20%251%24s&aoh=16301928057528&csi=0&referrer=https%3A%2F%2Fwww.google.com

In recent years, several computer scientists and physicists have been exploring the potential of quantum-enhanced machine learning algorithms. As their name suggests, quantum machine learning approaches combine quantum algorithms with machine learning techniques.

Most researchers investigating quantum machine learning algorithms have been trying to understand whether they could solve tasks faster than conventional machine learning techniques. One of the tasks that machine learning algorithms are commonly trained to complete are classification tasks, such as arranging images into different categories or accurately classifying specific objects or living creatures in an image.

Among the machine learning algorithms that achieved promising results in classification tasks are kernel methods, which include a renowned supervised learning technique called support-vector machine. Over the past few years, some scientists specialized in quantum algorithms have thus been exploring the potential of quantum kernel methods, which were first introduced by Havlicek and his colleagues at IBM.

Researchers at IBM Quantum have recently carried out a study further investigating the potential of quantum kernel methods. Their paper, published in *Nature Physics*, demonstrates that these methods could provide a robust quantum speed up over conventional kernel methods.

"Despite the popularity of quantum kernel methods, a fundamental question remained unanswered: Can quantum computers employ kernel methods to provide a provable advantage over classical learning algorithms?" Srinivasan Arunachalam, one of the researchers who carried out the study, told *Phys.org*. "Understanding this question was the starting point of our work. In this Nature Physics paper, along with my collaborators Yunchao Liu and Kristan Temme, we resolved this question in the affirmative."

As part of their study, Arunachalam and his colleagues constructed a classification problem that could be used to rigorously evaluate heuristic quantum kernel methods. Using this problem as an example, they proved the existence of a quantum kernel algorithm that can classify a set of points significantly faster than classical algorithms when trained on the same data and implemented on a fault-tolerance machine.

In the quantum kernel approach considered by the researchers a quantum computer steps in to run all the algorithm's computations, except for one specific portion. When given a set of classical data points, such as bit strings generated by a classical computer, the quantum kernel approach maps them into a higher dimensional space, where quantum computers can find patterns in data and extract characterizing features, using a technique called quantum kernel estimation (QKE).

"In order to use this technique for a separation between quantum and classical kernels, our starting point is a well-known problem that is often used to separate classical and quantum computing, the discrete logarithm problem," Arunachalam said. "This problem can be solved in polynomial time on a quantum computer using the famous Shor's algorithm but is strongly believed to require superpolynomial time for every classical algorithm."

Arunachalam and his colleagues were the first to construct a classification problem based on the hardness assumption of the discrete logarithm problem. Interestingly, they showed that the performance achieved by all classical machine learning techniques on this problem is worst or equal to random guessing, which is far from satisfactory.

"Subsequently, we constructed a kernel function that maps these classical data points onto a complex high dimensional feature space and show that QKE can solve this classification problem with very high precision in polynomial time," Arunachalam said. "An additional bonus is that we are able to show that this quantum speedup exists even if there is finite sampling noise while taking measurements, which is an important consideration for near-term and even fault-tolerant quantum computers."

Past studies have introduced several new quantum algorithms that could solve classification tasks faster than conventional machine learning techniques. However, most of these algorithms required strong input assumptions to achieve promising results or the researchers were unable to rigorously demonstrate their advantage over classical machine learning techniques.

"Our QKE algorithm can be viewed as an end-to-end quantum advantage for quantum kernel methods implemented on a fault-tolerant device (with realistic assumptions), since we start with classical data points and produce a classical solution for the classification problem using a quantum computer in the middle," Arunachalam said. "Of course, this is not the end of the road and instead only is reason to further understand quantum kernels better."

The recent work by this team of researchers provides a confirmation that quantum kernel methods could help to complete classification tasks faster and more efficiently. In their future studies, Arunachalam and his colleagues plan to investigate the potential of using these algorithms to tackle real world classification problems.

"The classification problem that we used to prove this advantage is artificially constructed to provide a theoretical underpinning for the usefulness of quantum kernels," Arunachalam said. "There is room to obtain further quantum speedups using quantum kernel methods for other (hopefully) practically relevant problems. We believe our result is interesting because it provides us with a direction to look for more learning problems that can benefit from kernel methods. In our future work we hope to understand how generalizable the structure of our classification problem is and if there are further speedups obtainable using similar structures."

# 7. Quantum computers could read all your encrypted data. This 'quantum-safe' VPN aims to stop that

by Daphne Leprince-Ringuet
https://www.zdnet.com/article/quantum-computers-could-read-all-our-encrypted-data-this-quantum-safe-vpn-is-trying-to-prevent-that/

To protect our private communications from future attacks by quantum computers, Verizon is trialing the use of next-generation cryptography keys to protect the virtual private networks (VPNs) that are used every day by companies around the world to prevent hacking.

Verizon implemented what it describes as a "quantum-safe" VPN between one of the company's labs in London in the UK and a US-based center in Ashburn, Virginia, using encryption keys that were generated thanks to post-quantum cryptography methods – meaning that they are robust enough to withstand attacks from a quantum computer.

According to Verizon, the trial successfully demonstrated that it is possible to replace current security processes with protocols that are quantum-proof.

VPNs are a common security tool used to protect connections made over the internet, by creating a private network from a public internet connection. When a user browses the web with a VPN, all of their data is redirected through a specifically configured remote server run by the VPN host, which acts as a filter that encrypts the information.

This means that the user's IP address and any of their online activities, from sending emails to paying bills, come out as gibberish to potential hackers – even on insecure networks like public WiFi, where eavesdropping is much easier.

Especially in the last few months, which have seen many employees switching to full-time working from home, VPNs have become an increasingly popular tool to ensure privacy and security on the internet.

The technology, however, is based on cryptography protocols that are not un-hackable. To encrypt data, VPN hosts use encryption keys that are generated by well-established algorithms such as RSA (Rivest–Shamir–Adleman). The difficulty of cracking the key, and therefore of reading the data, is directly linked to the algorithm's ability to create as complicated a key as possible.

In other words, encryption protocols as we know them are essentially a huge math problem for hackers to solve. With existing computers, cracking the equation is extremely difficult, which is why VPNs, for now, are still a secure solution. But quantum computers are expected to bring about huge amounts of extra computing power – and with that, the ability to hack any cryptography key in minutes.

"A lot of secure communications rely on algorithms which have been very successful in offering secure cryptography keys for decades," Venkata Josyula, the director of technology at Verizon, tells ZDNet. "But there is enough research out there saying that these can be broken when there is a quantum computer available at a certain capacity. When that is available, you want to be protecting your entire VPN infrastructure."

One approach that researchers are working on consists of developing algorithms that can generate keys that are too difficult to hack, even with a quantum computer. This area of research is known as post-quantum cryptography, and is particularly sought after by governments around the world.

In the US, for example, the National Institute of Standards and Technology (NIST) launched a global research effort in 2016 calling on researchers to submit ideas for algorithms that would be less susceptible to a quantum attack. A few months ago, the organization selected a group of 15 algorithms that showed the most promise.

"NIST is leading a standardization process, but we didn't want to wait for that to be complete because getting cryptography to change across the globe is a pretty daunting task," says Josyula. "It could take 10 or even 20 years, so we wanted to get into this early to figure out the implications."

Verizon has significant amounts of VPN infrastructure and the company sells VPN products, which is why the team started investigating how to start enabling post-quantum cryptography right now and in existing services, Josyula adds.

One of the 15 algorithms identified by NIST, called Saber, was selected for the test. **Saber** generated quantum-safe cryptography keys that were delivered to the endpoints – in London and Ashburn – of a typical IPsec VPN through an extra layer of infrastructure, which was provided by a third-party vendor.

Whether Saber makes it to the final rounds of NIST's standardization process, in this case, doesn't matter, explains Josyula. "We tried Saber here, but we will be trying others. We are able to switch from one algorithm to the other. We want to have that flexibility, to be able to adapt in line with the process of standardization."

In other words, Verizon's test has shown that it is possible to implement post-quantum cryptography candidates on infrastructure links now, with the ability to migrate as needed between different candidates for quantum-proof algorithms.

This is important because, although a large-scale quantum computer could be more than a decade away, there is still a chance that the data that is currently encrypted with existing cryptography protocols is at risk.

The threat is known as "harvest now, decrypt later" and refers to the possibility that hackers could collect huge amounts of encrypted data and sit on it while they wait for a quantum computer to come along that could read all the information.

"If it's your Amazon shopping cart, you may not care if someone gets to see it in ten years," says Josyula. "But you can extend this to your bank account, personal number, and all the way to government secrets. It's about how far into the future you see value for the data that you own – and some of these have very long lifetimes."

For this type of data, it is important to start thinking about long-term security now, which includes the risk posed by quantum computers.

A quantum-safe VPN could be a good start – even though, as Josyula explains, many elements still need to be smoothed out. For example, Verizon still relied on standard mechanisms in its trial to deliver quantum-proof keys to the VPN end-points. This might be a sticking point, if it turns out that this phase of the process is not invulnerable to quantum attack.

The idea, however, is to take proactive steps to prepare, instead of waiting for the worst-case scenario to happen. Connecting London to Ashburn was a first step, and Verizon is now looking at extending its quantum-safe VPN to other locations.

# 8. Toshiba Makes Breakthrough Towards the Quantum Internet

by Francisco Pires
https://www.tomshardware.com/news/toshiba-makes-breakthrough-towards-the-quantum-internet

Toshiba today announced a breakthrough on the road towards the quantum internet. In partnership with the Tohoku University Hospital (Japan), the team of researchers demonstrated the transmission of the entire human genome over 600 km of fiber optics - while encoding the information with quantum cryptography for the ultimate data privacy protection. The result of the research was published on the Nature Photonics scientific journal.

The data was moved and stored through several locations, spanning a total travel distance of around 600 km via fiber optics cables. A new, world-first dual band stabilisation technique was employed (the company has named it Twin Field), which helps in cancelling the problem of temperature and strain fluctuations usually present in quantum communications. This is pure physics: as data flows through optical cables, the cables themselves show diminutive contractions and expansions, which if not accounted for, can destabilize the extremely sensitive qubits used to encode and transmit the information - introducing errors in the data or even rendering it unusable. Toshiba's deployed dual band technique, as described by the company, "(...) sends two optical reference signals, at different wavelengths, for minimising the phase fluctuations on long fibres. The first wavelength is used to cancel the rapidly varying fluctuations, while the second wavelength, at the same wavelength as the optical qubits, is used for fine adjustment of the phase." The data was repeatedly verified at various stages of its journey through the network - and due to the new technique, showed no signs of degradation.

The research finally opens the door to long distance Quantum Key Distribution (QKD). QKD is essentially a distribution protocol for encryption keys, albeit based on quantum physics - and is being hailed as the final frontier in encryption schemas. This "final frontier of security" is being touted on the basis of quantum physics, and the behavior of qubits, themselves: after data has been encrypted with a secure QKD key, it can then be sent over an insecure connection (such as the internet), where only the holders of the decryption key can access its contents. Certain characteristics of the quantum realm are especially useful in guaranteeing security: for one, the basic quantum observation principle, which underpins much of quantum-bound research, states that the mere act of observing a flowing system will change its final result. Based on this, should the secure, QKD-encrypted communication be intercepted by a third party, the interception itself will induce changes into the flow of information, which can serve as a warning for the information sender (or receiver) that someone has attempted to tamper with and intercept the flow of data.

Andrew Shields, Head of the Quantum Technology Division at Toshiba Europe remarks, “QKD has been used to secure metropolitan area networks in recent years. This latest advance extends the maximum span of a quantum link, so that it is possible to connect cities across countries and continents, without using trusted intermediate nodes. Implemented along with Satellite QKD, it will allow us to build a global network for quantum secured communications.”

Another piece of investigation conducted by Toshiba includes multiplexing compatibility: this essentially allows both the data and the quantum keys to be transmitted on the same fibre, thus eliminating the need for a costly, dedicated infrastructure for key distribution.

# 9. IonQ Says New Architecture a Step Toward More Powerful Quantum Computers

by Matt Swayne
https://thequantumdaily.com/2021/08/26/ionq-says-new-architecture-a-step-toward-more-powerful-quantum-computers/

IonQ, Inc. unveiled a **Reconfigurable Multicore Quantum Architecture (RMQA)** technology, what the company termed a breakthrough in quantum computing. They added that are ahead of technical roadmap expectations at the start of 2021.

IonQ demonstrated achieving 4 chains of 16 ions each that can be dynamically configured into quantum computing cores. Company officials believe this has laid the foundation for increases to qubit count into the triple digits on a single chip, as well as future Parallel Multicore Quantum Processing Units.

This demonstration was achieved on a technological platform recently added to IonQ's list of intellectual property, called Evaporated Glass Traps (EGTs). Developed by an IonQ team led by UC Berkeley Physics PhD and ex-GTRI and -NIST researcher Jason Amini, the EGT platform offers an unprecedented level of performance and is a crucial part of IonQ's roadmap to rapid scalability and increased computing power.

"The Reconfigurable Multicore Quantum Architecture marks a key milestone for IonQ and for the quantum computing industry in general," remarked IonQ President and CEO Peter Chapman. "RMQA is a critical enabler of our ability to scale qubit density and deliver the computational power projected in our roadmap. We're very proud of the team at IonQ that has achieved a powerful platform for scalability and control in a single technical breakthrough."

Today's news involves the separation and merger of a total of 64 ions to create a RMQA using 4 chains of 16 ions each. The ion chains are transported and merged into permutations of a higher-connectivity, 32-ion quantum computing core, allowing for scaling to large numbers of qubits without the fidelity loss that historically accompanies very long chains of ions. This architecture was realized on IonQ's EGT Series ion trap chip, which provides the stability necessary to operate this architecture with little to no recalibration, maximizing uptime and optimizing transport. The EGT series platforms are expected to be extended to support more chains, with each chain increasing the quantum computational power by a factor of 4000 or more.

The news continues a year of considerable momentum for IonQ. Its trapped-ion quantum computers were recently added to Google Cloud Marketplace, making IonQ the only supplier whose quantum computers are available via all of the major cloud providers. In addition, IonQ's co-founders joined the White House's National Quantum Initiative Advisory Committee to accelerate the development of the national strategic technological imperative. IonQ is also preparing to become the first publicly-traded, pure-play quantum computing company via a merger with dMY Technology Group, Inc. III

# 10. The All-Seeing "i": Apple Just Declared War on Your Privacy

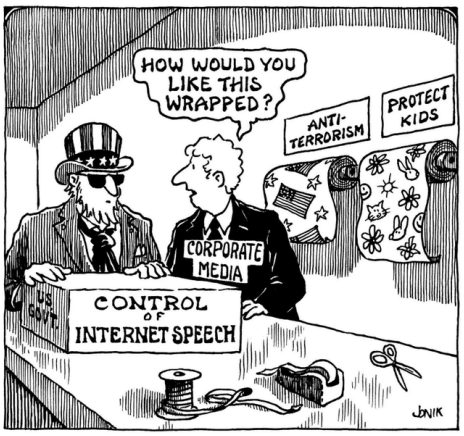
by Edward Snowden
https://edwardsnowden.substack.com/p/all-seeing-i?r=q0ig0

By now you've probably heard that Apple plans to push a new and uniquely intrusive surveillance system out to many of the more than *one billion* iPhones it has sold, which all run the behemoth's proprietary, take-it-or-leave-it software. This new offensive is tentatively slated to begin with the launch of iOS 15—almost certainly in mid-September—with the devices of its US user-base designated as the initial targets. We're told that other countries will be spared, but not for long.

You might have noticed that I haven't mentioned which problem it is that Apple is purporting to solve. Why? Because it doesn't matter.

Having read thousands upon thousands of remarks on this growing scandal, it has become clear to me that many understand it doesn't matter, but few if any have been willing to actually say it. Speaking candidly, if that's still allowed, that's the way it always goes when someone of institutional significance launches a campaign to defend an indefensible intrusion into our private spaces. They make a mad dash to the supposed high ground, from which they speak in low, solemn tones about their moral mission before fervently invoking the dread spectre of the Four Horsemen of the Infopocalypse, warning that only a dubious amulet—or suspicious software update—can save us from the most threatening members of our species.

Suddenly, everybody with a principled objection is forced to preface their concern with apologetic throat-clearing and bonafides: *I lost a friend when the towers came down, however... As a parent, I understand this is a real problem, but…*




As a parent, I'm here to tell you that sometimes it doesn't matter *why* the man in the handsome suit is doing something. What matters are the consequences.

Apple's new system, regardless of how anyone tries to justify it, will permanently redefine what belongs to you, and what belongs to them.

How?

The task Apple intends its new surveillance system to perform—preventing their cloud systems from being used to store digital contraband, in this case unlawful images uploaded by their customers—is traditionally performed by searching *their systems*. While it's still problematic for anybody to search through a billion people's private files, the fact that they can only see the files you gave them is a crucial limitation.

Now, however, that's all set to change. Under the new design, *your phone* will now perform these searches on Apple's behalf before your photos have even reached their iCloud servers, and—*yada, yada, yada*—if enough "forbidden content" is discovered, law-enforcement will be notified.

I intentionally wave away the technical and procedural details of Apple's system here, some of which are quite clever, because they, like our man in the handsome suit, merely distract from the most pressing fact—the fact that, in just a few weeks, Apple plans to erase the boundary dividing which devices work for you, and which devices work for them.

Why is this so important? Once the precedent has been set that it is fit and proper for even a "pro-privacy" company like Apple to make products that betray their users and owners, Apple itself will lose all control over how that precedent is applied. As soon as the public first came to learn of the "spyPhone" plan, experts began investigating its technical weaknesses, and the many ways it could be abused, primarily *within the parameters of Apple's design.* Although these valiant vulnerability-research efforts have produced compelling evidence that the system is seriously flawed, they also seriously miss the point: Apple gets to decide whether or not their phones will monitor their owners 'infractions for the government, but it's *the government* that gets to decide what constitutes an infraction... and how to handle it.

For its part, Apple says their system, in its initial, v1.0 design, has a narrow focus: it only scrutinizes photos intended to be uploaded to iCloud (although for 85% of its customers, that means ***EVERY*** photo), and it does not scrutinize them beyond a simple comparison against a database of specific examples of previously-identified child sexual abuse material (CSAM).

If you're an enterprising pedophile with a basement full of CSAM-tainted iPhones, Apple welcomes you to entirely exempt yourself from these scans by simply flipping the "Disable iCloud Photos" switch, a bypass which reveals that *this system was never designed to protect children*, as they would have you believe, but rather to protect their brand. As long as you keep that material off their servers, and so keep Apple out of the headlines, Apple doesn't care.

So what happens when, in a few years at the latest, a politician points that out, and—in order *to protect the children*—bills are passed in the legislature to prohibit this "Disable" bypass, effectively compelling Apple to scan photos that *aren't* backed up to iCloud? What happens when a party in India demands they start scanning for memes associated with a separatist movement? What happens when the UK demands they scan for a library of terrorist imagery? How long do we have left before the iPhone in your pocket begins quietly filing reports about encountering "extremist" political material, or about your presence at a "civil disturbance"? Or simply about your iPhone's possession of a video clip that contains, or maybe-or-maybe-not contains, a blurry image of a passer-by who resembles, according to an algorithm, "a person of interest"?

For its part, Apple says their system, in its initial, v1.0 design, has a narrow focus: it only scrutinizes photos intended to be uploaded to iCloud (although for 85% of its customers, that means ***EVERY*** photo), and it does not scrutinize

them beyond a simple comparison against a database of specific examples of previously-identified child sexual abuse material (CSAM).

If you're an enterprising pedophile with a basement full of CSAM-tainted iPhones, Apple welcomes you to entirely exempt yourself from these scans by simply flipping the "Disable iCloud Photos" switch, a bypass which reveals that *this system was never designed to protect children*, as they would have you believe, but rather to protect their brand. As long as you keep that material off their servers, and so keep Apple out of the headlines, Apple doesn't care.

So what happens when, in a few years at the latest, a politician points that out, and—in order *to protect the children*—bills are passed in the legislature to prohibit this "Disable" bypass, effectively compelling Apple to scan photos that *aren't* backed up to iCloud? What happens when a party in India demands they start scanning for memes associated with a separatist movement? What happens when the UK demands they scan for a library of terrorist imagery? How long do we have left before the iPhone in your pocket begins quietly filing reports about encountering "extremist" political material, or about your presence at a "civil disturbance"? Or simply about your iPhone's possession of a video clip that contains, or maybe-or-maybe-not contains, a blurry image of a passer-by who resembles, according to an algorithm, "a person of interest"?

One particular frustration for me is that I know some people at Apple, and I even like some people at Apple—bright, principled people who should know better. Actually, who *do* know better. Every security expert in the world is screaming themselves hoarse now, imploring Apple to stop, even those experts who in more normal circumstances reliably argue *in favor* of censorship. Even some survivors of child exploitation are against it. And yet, as the OG designer Galileo once said, it moves.

Faced with a blistering torrent of global condemnation, Apple has responded not by addressing any concerns or making any changes, or, more sensibly, by just scrapping the plan altogether, but by deploying their man-in-the-handsome-suit software chief, who resembles the well-moisturized villain from a movie about Wall Street, to give quotes to, yes, the *Wall Street Journal* about how sorry the company is for the "confusion" it has caused, but how the public shouldn't worry: Apple "feel[s] very good about what they're doing."

One particular frustration for me is that I know some people at Apple, and I even like some people at Apple—bright, principled people who should know better. Actually, who *do* know better. Every security expert in the world is screaming themselves hoarse now, imploring Apple to stop, even those experts who in more normal circumstances reliably argue *in favor* of censorship. Even some survivors of child exploitation are against it. And yet, as the OG designer Galileo once said, it moves.

Faced with a blistering torrent of global condemnation, Apple has responded not by addressing any concerns or making any changes, or, more sensibly, by just scrapping the plan altogether, but by deploying their man-in-the-handsome-suit software chief, who resembles the well-moisturized villain from a movie about Wall Street, to give quotes to, yes, the *Wall Street Journal* about how sorry the company is for the "confusion" it has caused, but how the public shouldn't worry: Apple "feel[s] very good about what they're doing."

This is the goal of end-to-end encryption: drawing a new and ineradicable line in the digital sand dividing *your* data and *their* data. It allows you to trust a service provider to *store* your data without granting them any ability to *understand* it. This would mean that even Apple itself could no longer be expected to rummage through your iCloud account with its grabby little raccoon hands—and therefore could not be expected to hand it over to any government that can stamp a sheet of paper, which is precisely why the FBI (again: secretly) complained.

For Apple to realize this original vision would have represented a *huge* improvement in the privacy of our devices, effectively delivering the final word in a thirty year-long debate over establishing a new industry standard—and, by

extension, the new global expectation that parties seeking access to data from a device must *obtain it* from that device, rather than turning the internet and its ecosystem into a spy machine.

Unfortunately, I am here to report that once again, the optimists are wrong: Apple's proposal to make their phones inform on and betray their owners marks the dawn of a dark future, one to be written in the blood of the political opposition of a hundred countries that will exploit this system to the hilt. See, the day after this system goes live, it will no longer matter whether or not Apple ever enables end-to-end encryption, because our iPhones will be reporting their contents *before our keys are even used*.

I can't think of any other company that has so proudly, and so publicly, distributed spyware to its own devices—and I can't think of a threat more dangerous to a product's security than the mischief of its own maker. There is no fundamental technological limit to how far the precedent Apple is establishing can be pushed, meaning the only restraint is Apple's all-too-flexible company policy, something governments understand all too well.

I would say there should be a law, but I fear it would only make things worse.

We are bearing witness to the construction of an all-seeing-**i**—an Eye of *Im*providence—under whose aegis *every iPhone will search itself* for whatever Apple wants, or for whatever Apple is directed to want. They are inventing a world in which every product you purchase owes its highest loyalty to someone other than its owner.

To put it bluntly, this is not an innovation but a tragedy, a disaster-in-the-making.

Or maybe I'm confused—or maybe I just *think different*.

# 11. Quantum computers will soon fit in your phone

by MAIJA PALMER
https://sifted.eu/articles/diamond-quantum-computer/

A quantum computer small enough to sit on your desk — or be embedded in a satellite, car or even a mobile phone — is no longer a pipe dream. The first such machines are actually starting to be delivered to early customers, thanks to advances in qubits created using synthetic diamonds.

The technology received a vote of confidence from investors today, as 2 -year-old stealth startup Quantum Brilliance raised a nearly $10m seed funding round from a consortium of investors led by Main Sequence Ventures and the founders of QxBranch, the Australian quantum services company acquired by Rigetti.

The funding will speed the commercialisation of the technology, which Andrew Horsley, CEO of the Australian-German startup, says could dramatically change the way quantum computing can be used.

"It is simplifying the quantum computer and turning it into something that can sit in an ordinary server rack next to classical computers. Most quantum computers are giant mainframes; these will eventually be small enough to be embedded in mobile devices," Horsley told Sifted. "The miniaturisation potential is huge."

So is the volume of quantum computers that could be created using this technique.

We are thinking about volumes in millions, not the thousands that people talk about with quantum computers based on superconducting," said Marcus Doherty, chief science officer.

Quantum Brilliance delivered its first system to the Pawsey Supercomputing Centre in Australia earlier this year and is beginning to ship to other commercial customers.

## Room-temperature quantum computers

Quantum Brilliance is developing quantum computers based on synthetic diamonds, which don't need temperatures close to absolute zero or complex laser systems to operate. It is in stark contrast to the superconducting quantum systems developed by big companies like Google, IBM and Rigetti which need large and energy-hungry cooling systems to keep them at a temperature colder than interstellar space.

Trapped ion computing systems, such as those created by Honeywell and IonQ, have the potential to be smaller, but even the smallest such computer, unveiled by a research team from the University of Innsbruck this summer, was the size of two server racks.

In contrast, Quantum Brilliance's system is the size of a lunchbox.

The quality of diamond-based qubits is somewhere between that of superconducting qubits and trapped-ion qubits.

"It is middle of the pack for performance," Doherty told Sifted. The gate speeds are slower than for superconducting qubits, but faster than trapped ions. The coherence of the diamond qubits is lower than those of trapped ions. The big advantage, however, is being able to run at room temperature.

The Quantum Brilliance quantum accelerators have only two qubits at the moment, paltry compared to the 72-qubit systems that Google has developed. Horsley said, however, that the company can reach 50 qubits by 2025.

## How it works

Diamond-based qubits are created using diamonds with a specific defect — one carbon atom of the diamond lattice is replaced by a nitrogen atom, with a gap left next to it. The gap, or vacancy, becomes negatively charged and behaves like a trapped ion. This can be manipulated into a qubit when lit with a green laser. (Synthetic diamonds are being developed for various high-tech purposes like this.)

Diamond-based qubits were a leading idea in quantum computing until around 2014, says Doherty, but progress halted because it proved hard to create synthetic diamonds with enough precision to make the system workable. The Quantum Brilliance cofounders 'breakthrough was developing a novel fabrication technique that allows greater precision. The startup buys synthetic diamonds from Element Six, the synthetic diamond manufacturer, part of the De Beers Group, and then carries out the final part of the fabrication process in house.

Quantum Brilliance was spun out from the Australian National University in 2019 and only recently emerged from stealth mode. It now has 25 staff and is actively hiring for 20 more roles. The startup is aiming to grow to more than 100 staff in the next year, half of which will be based in Germany.

The company is in the process of establishing an office in Germany, in part to capitalise on the €2bn in funding that the German government has pledged for the quantum computing sector, and also to take advantage of a skilled work-force

"Germany has one of the highest densities of diamond quantum research groups, and also expertise in precision man-ufacturing," said Horsley. Big car manufacturers, which are expected to be some of the first quantum computing customers, are also clustered in the region.

### Is this the end of other types of quantum computer?

Will room-temperature quantum computing completely eclipse the other, bulkier approaches like superconducting? Not immediately, says Doherty.

"The future is heterogeneous — the idea of a single computer that can do everything is gone," he said. Quantum computers, especially when they still have just a few qubits, are likely to be heavily tailored to solving one particular problem. Speedier quantum computers — for example, superconducting systems — may be used for one type of problem, while diamond-based ones are used for another.

Calculations involving a single, complex molecule, for example, may be more appropriate to crunch on a mainframe in a lab. But a network of smaller diamond-based machines, processing in parallel, could be better at calculating how systems of small molecules all interact with each other.

Over time as qubit counts go up, however, Doherty is expecting the quantum computing mix to shift in favour of diamonds. "Over time some technologies will fade out. The ultimate endpoint for us is to be the quantum computer for everything."

# 12. Glass Chip Is Key to New Quantum Architecture

by SAMUEL K. MOORE
https://spectrum.ieee.org/ionq-new-quantum-computing-chip

Maryland-based IonQ has unveiled a new kind of chip in its quest to scale up its type of quantum computer technology. Its computers calculate using the quantum states of ions electromagnetically trapped in the space near a chip. Previous traps were made using silicon chipmaking processes, but the company has now switched to an evaporated glass trap technology—a way of constructing micrometer-scale features in fused silica glass often used to make microfluidic chips. Its previous trap technology, the company says, could not have supported IonQ's new quantum architecture, which is based on multiple chains of ion-based qubits. Ultimately, IonQ executives say, the glass chip's reconfigurable chains of ions will allow for computers with qubits that number in the triple digits.

"The purpose of an ion trap is to move ions around with precision, hold them in the environment, and get out of the way of the quantum operation," explains Jason Amini, who led the evaporated glass trap team at IonQ. The 3D glass and metal structure Amini's team constructed does all three better than its previous chips could, Amini says. Stray electric fields from charge on the silicon-based chip could destabilize the ions' delicate quantum states, reducing the

fidelity of quantum computation. But the evaporated glass design "hides any material that could hold charge," he says. The effect is a more stable trap that computes better.

Another advantage, Amini says, is that the trap could be shaped to "get out of the way" of quantum operations. In an ion trap computer the ions' quantum states are manipulated by zapping them with lasers. "We have to bring a lot of laser beams over the surface," says Amini. The glass chip is "shaped to allow lasers to come through and address the device."

IonQ previously had silicon ion traps constructed at Sandia National Laboratory in New Mexico. But IonQ wanted more control over the technology and the ability to iterate designs faster, says CEO Peter Chapman.

With the evaporated glass ion trap in hand, IonQ proceeded with a demonstration of their new quantum computing scheme, which Chapman calls the industry's first "reconfigurable multicore quantum architecture", or RMQA. But don't look for too many parallels between field programmable gate arrays and multicore CPUs.

In IonQ's demonstration it works like this: The trap holds four separate chains of 16 ions in a line. Each chain can be moved into position to be manipulated by the lasers, altering their quantum state or entangling groups of ions so their quantum states are linked. "Each chain is, by itself, a quantum computer," says Chapman. In addition, two chains can be brought together to form a core that allows entangling qubits across the chains (the reconfiguration part) until eventually all the qubits can be linked to perform big, complex quantum operations.

It's not perfect, of course. Out of 16 ions, the technology produces 12 qubits, Chapman explains. (The other four are "refrigerant" ions that correct for imperfections during ion transport.) So IonQ's latest demonstration produce 48 qubits. But it is easily expanded by lengthening the trap. And, because this is quantum computing, a little expansion goes a long way, adding substantially more capability with each added qubit.

"The architecture allows you to relatively easily expand to hundreds of qubits on a single chip," says Chapman.

The next big leap will come from photonic interconnects IonQ is developing to link qubits on one chip to those on another. "Once you do entanglement, distance no longer matters," says Chapman. "Whether or not it's multiple chains on a chip or one chip to another, it all acts as if it's one big quantum computer."

# 13. Now is the time to prepare for the quantum computing revolution

by Karen Roby
https://www.techrepublic.com/article/expert-now-is-the-time-to-prepare-for-the-quantum-computing-revolution/?utm_medium=email&_hsmi=154123099&_hsenc=p2ANqtz-8RX7fz1RVmTpYVHc-coiJqqak9BXLIzY8LfhW6BVXo3Ari3q0SHYu2km9vpW3iF585KeMSvG0qsDR64rNbSYC3NCii4uw&utm_content=154123099&utm_source=hs_email

TechRepublic's Karen Roby spoke with Christopher Savoie, CEO and co-founder of Zapata Computing, a quantum application company, about the future of quantum computing. The following is an edited transcript of their conversation.

**Christoper Savoie:** There are two types of quantum-computing algorithms if you will. There are those that will require what we call a fault-tolerant computing system, one that doesn't have error, for all intents and purposes, that's corrected for error, which is the way most classical computers are now. They don't make errors in their calculations, or at least we hope they don't, not at any significant rate. And eventually we'll have these fault-tolerant quantum computers. People are working on it. We've proven that it can happen already, so that is down the line. But it's in the five- to 10-year range that it's going to take until we have that hardware available. But that's where a lot of the promises for these exponentially faster algorithms. So, these are the algorithms that will use these fault-tolerant computers to basically look at all the options available in a combinatorial matrix.

So, if you have something like Monte Carlo simulation, you can try significantly all the different variables that are possible and look at every possible combination and find the best optimal solution. So, that's really, practically impossible on today's classical computers. You have to choose what variables you're going to use and reduce things and take shortcuts. But with these fault-tolerant computers, for significantly many of the possible solutions in the solution space, we can look at all of the combinations. So, you can imagine almost an infinite amount or an exponential amount of variables that you can try out to see what your best solution is. In things like CCAR [Comprehensive Capital Analysis and Review], Dodd-Frank [Dodd-Frank Wall Street Reform and Consumer Protection Act] compliance, these things where you have to do these complex simulations, we rely on a Monte Carlo simulation.

So, trying all of the possible scenarios. That's not possible today, but this fault tolerance will allow us to try significantly all of the different combinations, which will hopefully give us the ability to predict the future in a much better way, which is important in these financial applications. But we don't have those computers today. They will be available sometime in the future. I hate putting a date on it, but think about it on the decade time horizon. On the other hand, there are these nearer-term algorithms that run on these noisy, so not error-corrected, noisy intermediate-scale quantum devices. We call them NISQ for short. And these are more heuristic types of algorithms that are tolerant to noise, much like neural networks are today in classical computing and [artificial intelligence] AI. You can deal a little bit with the sparse data and maybe some error in the data or other areas of your calculation. Because it's an about-type of calculation like neural networks do. It's not looking at the exact answers, all of them and figuring out which one is definitely the best. This is an approximate algorithm that iterates and tries to get closer and closer to the right answer.

But we know that neural networks work this way, deep neural networks. AI, in its current state, uses this type of algorithm, these heuristics. Most of what we do in computation nowadays and finance is heuristic in its nature and statistical in its nature, and it works good enough to do some really good work. In algorithmic trading, in risk analysis, this is what we use today. And these quantum versions of that will also be able to give us some advantage and maybe an advantage over—we've been able to show in recent work—the purely classical version of that. So, we'll have some quantum-augmented AI, quantum-augmented [machine learning] ML. We call it a quantum-enhanced ML or quantum-enhanced optimization that we'll be able to do.

So, people think of this as a dichotomy. We have these NISQ machines, and they're faulty, and then one day we'll wake up and we'll have this fault tolerance, but it's really not that way. These faulty algorithms, if you will, these heuristics that are about, they will still work and they may work better than the fault-tolerant algorithms for some problems and some datasets, so this really is a gradient. It really is. You'd have a false sense of solace, maybe two. "Oh well, if that's 10 years down the road we can just wait and let's wait till we wake up and have fault tolerance." But really the algorithms are going to be progressing. And the things that we develop now will still be useful in that fault-tolerant regime. And the patents will all be good for the stuff that we do now.

So, thinking that, "OK, this is a 10 year time horizon for those fault-tolerant computers. Our organization is just going to wait." Well, if you do, you get a couple of things. You're not going to have the workforce in place to be able to take advantage of this. You're probably not going to have the infrastructure in place to be able to take advantage of this. And meanwhile, all of your competitors and their vendors have acquired a portfolio of patents on these methodologies that are good for 20 years. So, if you wait five years from now and there's a patent four years down the line, that's good for 24 years. So there really is, I think, an incentive for organizations to really start working, even in this NISQ, this noisier regime that we're in today.

**Karen Roby:** You get a little false sense of security, as you mentioned, of something, oh, you say that's 10 years down the line, but really with this, you don't have the luxury of catching up if you wait too long. This is something that people need to be focused on now for what is down the road.

**Christoper Savoie:** Yes, absolutely. And in finance, if you have a better ability to detect risks then than your competitors; you're at a huge advantage to be able to find alpha in the market. If you can do that better than others, you're going to be at a huge advantage. And if you're blocked by people's patents or blocked by the fact that your workforce doesn't know how to use these things, you're really behind the eight ball. And we've seen this time and time again with different technology evolutions and revolutions. With big data and our use of big data, with that infrastructure, with AI and machine learning. The organizations that have waited generally have found themselves behind the eight ball, and it's really hard to catch up because this stuff is changing daily, weekly, and new inventions are happening. And if you don't have a workforce that's up and running and an infrastructure ready to accept this, it's really hard to catch up with your competitors.

**Karen Roby:** You've touched on this a little bit, but really for the finance industry, this can be transformative, really significant what quantum computing can do.

**Christoper Savoie:** Absolutely. At the end of the day, finance is math, and we can do better math and more accurate math on large datasets with quantum computing. There is no question about that. It's no longer an "if." Google has, with their experiment, proven that at some point we're going to have a machine that is definitely going to be better at doing math, some types of math, than classical computers. With that premise, if you're in a field that depends on math, that depends on numbers, which is everything, and statistics, which is finance, no matter what side you're on. If you're on the risk side or the investing side, you're going to need to have the best tools. And that doesn't mean you have to be an algorithmic trader necessarily, but even looking at tail risk and creating portfolios and this kind of thing. You're dependent on being able to quickly ascertain what that risk is, and computing is the only way to do that.

And on the regulatory side, I mentioned CCAR. I think as these capabilities emerge, it allows the regulators to ask for even more scenarios to be simulated, those things that are a big headache for a lot of companies. But it's important because our global financial system depends on stability and predictability, and to be able to have a computational resource like quantum that's going to allow us to see more variables or more possibilities or more disaster scenarios. It can really help. "What is the effect of, say, a COVID-type event on the global financial system?" To be more predictive of that and more accurate at doing that is good for everybody. I think all boats rise, and quantum is definitely going to give us that advantage as well.

**Karen Roby:** Most definitely. And Christopher, before I let you go, if you would just give us a quick snapshot of Zapata Computing and the work that you guys do.

**Christoper Savoie:** We have two really important components to try and make this stuff reality. On the one hand, we've got over 30 of the brightest young minds and algorithms, particularly for these near-term devices and how to write those. We've written some of the fundamental algorithms that are out there to be used on quantum computers. On the other hand, how do you make those things work? That's a software engineering thing. That's not really quantum

science. How do you make the big data work? And that's all the boring stuff of ETL and data transformation and digitalization and cloud and multicloud and all this boring but very important stuff. So basically Zapata is a company that has the best of the algorithms, but also best-of-breed means of actually software engineering that in a modern, multicloud environment that particularly finance companies, banks, they're regulated companies with a lot of data that is sensitive and private and proprietary. So, you need to be able to work in a safe and secure multicloud environment, and that's what our software engineering side allows us to do. We have the best of both worlds there.

# 14. A Peculiar State of Matter in Layers of Semiconductors Could Advance Quantum Computing

by MATTHEW HUTSON
https://scitechdaily.com/a-peculiar-state-of-matter-in-layers-of-semiconductors-could-advance-quantum-computing/

Scientists around the world are developing new hardware for quantum computers, a new type of device that could accelerate drug design, financial modelling, and weather prediction. These computers rely on qubits, bits of matter that can represent some combination of 1 and 0 simultaneously. The problem is that qubits are fickle, degrading into regular bits when interactions with surrounding matter interfere. But new research at MIT suggests a way to protect their states, using a phenomenon called many-body localization (MBL).

MBL is a peculiar phase of matter, proposed decades ago, that is unlike solid or liquid. Typically, matter comes to thermal equilibrium with its environment. That's why soup cools and ice cubes melt. But in MBL, an object consisting of many strongly interacting bodies, such as atoms, never reaches such equilibrium. Heat, like sound, consists of collective atomic vibrations and can travel in waves; an object always has such heat waves internally. But when there's enough disorder and enough interaction in the way its atoms are arranged, the waves can become trapped, thus preventing the object from reaching equilibrium.

MBL had been demonstrated in "optical lattices," arrangements of atoms at very cold temperatures held in place using lasers. But such setups are impractical. MBL had also arguably been shown in solid systems, but only with very slow temporal dynamics, in which the phase's existence is hard to prove because equilibrium might be reached if researchers could wait long enough. The MIT research found a signatures of MBL in a "solid-state" system — one made of semiconductors — that would otherwise have reached equilibrium in the time it was watched.

"It could open a new chapter in the study of quantum dynamics," says Rahul Nandkishore, a physicist at the University of Colorado at Boulder, who was not involved in the work.

Mingda Li, the Norman C Rasmussen Assistant Professor Nuclear Science and Engineering at MIT, led the new study, published in a recent issue of *Nano Letters*. The researchers built a system containing alternating semiconductor layers, creating a microscopic lasagna — aluminum arsenide, followed by gallium arsenide, and so on, for 600 layers, each 3 nanometers (millionths of a millimeter) thick. Between the layers they dispersed "nanodots," 2-nanometer particles of erbium arsenide, to create disorder. The lasagna, or "superlattice," came in three recipes: one with no nanodots, one in which nanodots covered 8 percent of each layer's area, and one in which they covered 25 percent.

According to Li, the team used layers of material, instead of a bulk material, to simplify the system so dissipation of heat across the planes was essentially one-dimensional. And they used nanodots, instead of mere chemical impurities, to crank up the disorder.

To measure whether these disordered systems are still staying in equilibrium, the researchers measured them with X-rays. Using the Advanced Photon Source at Argonne National Lab, they shot beams of radiation at an energy of more than 20,000 electron volts, and to resolve the energy difference between the incoming X-ray and after its reflection off the sample's surface, with an energy resolution less than one one-thousandth of an electron volt. To avoid penetrating the superlattice and hitting the underlying substrate, they shot it at an angle of just half a degree from parallel.

Just as light can be measured as waves or particles, so too can heat. The collective atomic vibration for heat in the form of a heat-carrying unit is called a phonon. X-rays interact with these phonons, and by measuring how X-rays reflect off the sample, the experimenters can determine if it is in equilibrium.

The researchers found that when the superlattice was cold — 30 kelvin, about -400 degrees Fahrenheit — and it contained nanodots, its phonons at certain frequencies remained were not in equilibrium.

More work remains to prove conclusively that MBL has been achieved, but "this new quantum phase can open up a whole new platform to explore quantum phenomena," Li says, "with many potential applications, from thermal storage to quantum computing."

To create qubits, some quantum computers employ specks of matter called quantum dots. Li says quantum dots similar to Li's nanodots could act as qubits. Magnets could read or write their quantum states, while the many-body localization would keep them insulated from heat and other environmental factors.

In terms of thermal storage, such a superlattice might switch in and out of an MBL phase by magnetically controlling the nanodots. It could insulate computer parts from heat at one moment, then allow parts to disperse heat when it won't cause damage. Or it could allow heat to build up and be harnessed later for generating electricity.

Conveniently, superlattices with nanodots can be constructed using traditional techniques for fabricating semiconductors, alongside other elements of computer chips. According to Li, "It's a much larger design space than with chemical doping, and there are numerous applications."

"I am excited to see that signatures of MBL can now also be found in real material systems," says Immanuel Bloch, scientific director at the Max-Planck-Institute of Quantum Optics, of the new work. "I believe this will help us to better understand the conditions under which MBL can be observed in different quantum many-body systems and how possible coupling to the environment affects the stability of the system. These are fundamental and important questions and the MIT experiment is an important step helping us to answer them."

# 15. Opening a path toward quantum computing in real-world conditions

by University of Virginia School of Engineering and Applied Science
https://www.sciencedaily.com/releases/2021/08/210820153706.htm

Drug discovery is one example. To understand drug interactions, a pharmaceutical company might want to simulate the interaction of two molecules. The challenge is that each molecule is composed of a few hundred atoms, and scientists must model all the ways in which these atoms might array themselves when their respective molecules are introduced. The number of possible configurations is infinite -- more than the number of atoms in the entire universe. Only a quantum computer can represent, much less solve, such an expansive, dynamic data problem.

Mainstream use of quantum computing remains decades away, while research teams in universities and private industry across the globe work on different dimensions of the technology.

A research team led by Xu Yi, assistant professor of electrical and computer engineering at the University of Virginia School of Engineering and Applied Science, has carved a niche in the physics and applications of photonic devices, which detect and shape light for a wide range of uses including communications and computing. His research group has created a scalable quantum computing platform, which drastically reduces the number of devices needed to achieve quantum speed, on a photonic chip the size of a penny.

Olivier Pfister, professor of quantum optics and quantum information at UVA, and Hansuek Lee, assistant professor at the Korean Advanced Institute of Science and Technology, contributed to this success.

*Nature Communications* recently published the team's experimental results, A Squeezed Quantum Microcomb on a Chip. Two of Yi's group members, Zijiao Yang, a Ph.D. student in physics, and Mandana Jahanbozorgi, a Ph.D. student of electrical and computer engi neering, are the paper's co-first authors. A grant from the National Science Foundation's Engineering Quantum Integrated Platforms for Quantum Communication program supports this research.

Quantum computing promises an entirely new way of processing information. Your desktop or laptop computer processes information in long strings of bits. A bit can hold only one of two values: zero or one. Quantum computers process information in parallel, which means they don't have to wait for one sequence of information to be processed before they can compute more. Their unit of information is called a qubit, a hybrid that can be one and zero at the same time. A quantum mode, or qumode, spans the full spectrum of variables between one and zero -- the values to the right of the decimal point.

Researchers are working on different approaches to efficiently produce the enormous number of qumodes needed to achieve quantum speeds.

Yi's photonics-based approach is attractive because a field of light is also full spectrum; each light wave in the spectrum has the potential to become a quantum unit. Yi hypothesized that by entangling fields of light, the light would achieve a quantum state.

You are likely familiar with the optical fibers that deliver information through the internet. Within each optical fiber, lasers of many different colors are used in parallel, a phenomenon called multiplexing. Yi carried the multiplexing concept into the quantum realm.

*Micro* is key to his team's success. UVA is a pioneer and a leader in the use of optical multiplexing to create a scalable quantum computing platform. In 2014, Pfister's group succeeded in generating more than 3,000 quantum modes in a bulk optical system. However, using this many quantum modes requires a large footprint to contain the thousands of mirrors, lenses and other components that would be needed to run an algorithm and perform other operations.

"The future of the field is integrated quantum optics," Pfister said. "Only by transferring quantum optics experiments from protected optics labs to field-compatible photonic chips will *bona fide* quantum technology be able to see the light of day. We are extremely fortunate to have been able to attract to UVA a world expert in quantum photonics such as Xu Yi, and I'm very excited by the perspectives these new results open to us."

Yi's group created a quantum source in an optical microresonator a ring-shaped, millimeter-sized structure that envelopes the photons and generates a microcobe, a device that efficiently converts photons from single to multiple wavelengths. Light circulates around the ring to build up optical power. This power buildup enhances chances for photons to interact, which produces quantum entanglement between fields of light in the microcomb.

Through multiplexing, Yi's team verified the generation of 40 qumodes from a single microresonator on a chip, proving that multiplexing of quantum modes can work in integrated photonic platforms. This is just the number they are able to measure.

"We estimate that when we optimize the system, we can generate thousands of qumodes from a single device," Yi said.

Yi's multiplexing technique opens a path toward quantum computing for real-world conditions, where errors are inevitable. This is true even in classical computers. But quantum states are much more fragile than classical states.

The number of qubits needed to compensate for errors could exceed one million, with a proportionate increase in the number of devices. Multiplexing reduces the number of devices needed by two or three orders of magnitude.

Yi's photonics-based system offers two additional advantages in the quantum computing quest. Quantum computing platforms that use superconducting electronic circuits require cooling to cryogenic temperatures. Because the photon has no mass, quantum computers with photonic integrated chips can run or sleep at room temperature. Additionally, Lee fabricated the microresonator on a silicon chip using standard lithography techniques. This is important because it implies the resonator or quantum source can be mass-produced.

"We are proud to push the frontiers of engineering in quantum computing and accelerate the transition from bulk optics to integrated photonics," Yi said. "We will continue to explore ways to integrate devices and circuits in a photonics-based quantum computing platform and optimize its performance."

# 16. OSU cryptography research leads to huge efficiency gain in secure computing

by Steve Lundeberg
https://techxplore.com/news/2021-08-osu-cryptography-huge-efficiency-gain.html

Oregon State University researchers have developed a secure computation protocol that's 25% more efficient than what had been thought the best possible, meaning future savings in time and energy costs for groups needing to team up on computations while keeping their individual data private.

Mike Rosulek, associate professor of computer science in the OSU College of Engineering, and graduate student Lance Roy presented their findings at this month's virtual 41st annual International Cryptology Conference, or Crytpo 2021. The conference is organized by the International Association for Cryptologic Research.

Roy, a 22-year-old who grew up in Corvallis, entered Oregon State's computer science Ph.D. program at 18, going directly from homeschool high school to the OSU Graduate School. He had begun auditing undergraduate courses at OSU at age 12.

Secure computation is often explained via "Yao's millionaire problem," a hypothetical situation developed by and named after computer scientist and computational theorist Andrew Yao in which two wealthy people want to determine who is richer but neither wants to reveal to the other how much money she/he has.

"In real life, companies and other groups will agree on a computation to run, then they do some cryptographic magic, and at the end they learn only the final result of the computation—the inputs and intermediate results of the computation remain private," Rosulek said. "One of my favorite examples is the city of Boston wanting to answer the question of whether there was a gender-based wage gap in the city's tech sector. The tech companies collectively computed the relevant aggregate statistics on their combined payroll data, but without any company needing to reveal its payroll data."

A standard technique within secure computation protocols is garbled circuits, which can come in multiple constructions. Garbled circuits are one of the few ways to achieve general-purpose secure computation protocols with just a few rounds of communication among the parties involved, Rosulek explains.

"The most efficient construction of garbled circuits is from one of my previous papers, in 2015," said Rosulek, whose Twitter handle is @GarbledCircus. "In that paper we also gave some good evidence that this was as efficient as you could get. I really believed it was not possible to do better, and since 2015 I have been trying to prove conclusively that it was impossible to do better. This latest result was a big surprise because we showed how to actually do 25% better than that 2015 paper."

Rosulek describes Roy as the "mastermind" behind the more efficient garbled circuits, which involve insights they've named "slicing and dicing."

"I had stopped devoting any thought to trying to do better than what we did in the 2015 paper," Rosulek said. "Lance was familiar with this problem but it wasn't something we were actively working on together. I was very skeptical

when Lance came to me with an out-of-the-box idea, but it turns out that his instincts were correct and he soon convinced me that his crazy new idea worked."

A normal computer circuit, Roy explains, contains gates that perform basic computations on data. In a garbled circuit, the gates have been modified—garbled—so the data flowing through them is encrypted.

In trying to prove the 2015 garbled circuit technique could not be improved upon, Roy found his proof idea was valid if a gate used all of the information contained in an input, or none of it, but not if it used some of it. That concept, slicing, shifted his thinking toward trying to improve on the 2015 technique rather than prove it couldn't be made better.

"However, I also had a new problem," Roy said. "The way that slicing works, it'd leak too much information for the garbled circuits to be secure."

A year or so later, in late summer 2020, he came up with a solution: dicing.

"If the way the garbled circuits were built was randomized—i.e., by rolling the dice—and some other information was kept secret, the slicing idea could be made secure," he said. "Mike was really excited when I showed it to him, and during winter 2021 we refined the technique and wrote up the result."

# 17. Proposal for space-borne quantum memories for global quantum networking

by Mustafa Gündoğan, Jasminder S. Sidhu, Victoria Henderson, Luca Mazzarella, Janik Wolters, Daniel K. L. Oi & Markus Krutzik
https://www.nature.com/articles/s41534-021-00460-9

Global-scale quantum communication links will form the backbone of the quantum internet. However, exponential loss in optical fibres precludes any realistic application beyond few hundred kilometres. Quantum repeaters and space-based systems offer solutions to overcome this limitation. Here, we analyse the use of quantum memory (QM)-equipped satellites for quantum communication focussing on global range repeaters and memory-assisted (MA-) QKD, where QMs help increase the key rate by synchronising otherwise probabilistic detection events. We demonstrate that satellites equipped with QMs provide three orders of magnitude faster entanglement distribution rates than existing protocols based on fibre-based repeaters or space systems without QMs. We analyse how entanglement distribution performance depends on memory characteristics, determine benchmarks to assess the performance of different tasks and propose various architectures for light-matter interfaces. Our work provides a roadmap to realise unconditionally secure quantum communications over global distances with near-term technologies.

# 18. Abu Dhabi Starts Work on Quantum Computer, Just The Start of The Country's Long-Term Quantum Plan

by Matt Swayne
https://thequantumdaily.com/2021/08/18/abu-dhabi-starts-work-on-quantum-computer-just-the-start-of-the-countrys-long-term-quantum-plan/

Abu Dhabi, highly regarded as a global economic powerhouse, is now well on its way to becoming a quantum powerhouse.

The National, a UAE paper, reports that the Technology Innovation Institute, an Abu Dhabi government funded research institution, have begun building the region's first quantum computer.

"This will put the UAE on the map to be a known entity for research on such a topic. And that's a big achievement for the entire Arab world," Boulos Alfakes, a senior researcher, told the newspaper.

The institute's engineers are busy building the device. The newspaper reports that two dilution refrigerators arrived from Finland. Emirates Global Aluminium, an Abu Dhabi firm, provided the aluminium that will hold the quantum chip.

In March 2021, the QRC announced its devices will use superconducting qubits, similar to Google and IBM technology, saying that the approach offers the best qubit technology to scale to a larger quantum computer.

According to professor Jose Ignacio Latorre, the chief of research at the Quantum Research Centre, building a quantum computer is just the first step. He sees this as a part of a long-term vision to develop leadership in advanced technology, which will be "critical to national security and economic development."

He told The National News, "There will be a dramatic difference between the countries that own the technology and the ones that depend on the technology. The Emirates, like Singapore or Israel, [countries] of comparable sizes, cannot depend fully on allies. They have to develop their own technological strategies and they have to be sovereign. That is fundamental."

UAE scientists are also planning to engage in research on applications such as quantum algorithms for artificial intelligence and drug discovery, a new generation of navigation devices and cryptography that will make data safer in a post-quantum world, according to the paper.

Latorre added that building a quantum computer will be "useless" without education and talent development.

"We have to engage the country as a whole," Latorre said. "We need companies, oil and gas, telecommunications, so when a new technology comes, you [are] ready for that … these efforts should merge with efforts at universities and should also engage industry. The more educated people are, the more reasonable our planet should be."

In an editorial, the National News said the agenda is more than just a quantum nationalism muscle flex, but to create technologies to help science and society.

The editors write: "The assembly of this supercomputer, at the Technology Innovation Institute (TII), represents the beginning of a journey that is vital for the UAE not only to safeguard its strategic interests, but also to help solve the most urgent problems confronting humankind."

# 19. Xanadu and imec Partner to Develop Photonic Chips for Fault Tolerant Quantum Computing

by Matt Swayne
https://thequantumdaily.com/2021/08/18/xanadu-and-imec-partner-to-develop-photonic-chips-for-fault-tolerant-quantum-computing/

Xanadu, a full-stack photonic quantum computing company and imec, a world-leading research and innovation center in nanoelectronics and digital technologies, have today announced a partnership to develop the next generation of photonic qubits based on ultra-low loss silicon nitride (SiN) waveguides.

Xanadu is developing a unique type of quantum computer, one based on photonics. Specifically, these photonic qubits are based on squeezed states – a special type of light generated by chip-integrated silicon photonic devices. Such an approach uses particles of light to carry information through photonic chips, rather than electrons or ions used by other approaches. Xanadu's photonic approach offers the benefits of scalability to one million qubits via optical networking, room temperature computation, and the natural ability to leverage fabrication R&D centers such as imec.

"One of the most critical challenges in building a photonic quantum computer is finding the right fabrication partner that can simultaneously deliver cutting-edge process development and volume production of high performing photonic chips," said Zachary Vernon, who heads up Xanadu's Hardware team. "Imec is one of the few semiconductor R&D centers that does advanced technology R&D on advanced 200mm and 300mm lines, as well as volume manufacturing on their 200mm line, capable of delivering up to a thousand wafers per year per customer on a few platforms including ultralow-loss photonic platforms. The seamless transfer offered by imec of new processes to production is especially critical for rapid scaling of our technology."

Competing platforms for photonic quantum computing traditionally rely on single photon sources made from silicon waveguides, which suffer from non-deterministic operation. Using silicon nitride enables the generation of squeezed states, which replace single photons as the basic resource for synthesizing qubits. Squeezed states are deterministically generated, and can be used to distill error-resistant qubits called 'GKP states'. When multiplexed and implemented in Xanadu's architecture, these offer a more promising path to fault-tolerant quantum computing.

Amin Abbasi, business development manager at imec: "We are pleased to see that imec's wafer-scale low loss SiN photonics platform, initially developed for communication, is finding its way towards other advanced applications, like quantum computing. We look forward to working with Xanadu to drive further development of this platform for their particular needs."

"We are pleased to partner with Xanadu, one of the most exciting companies working in the quantum computing space." said Philippe Helin, specialty components program manager at imec.

"Xanadu's mission to build photonic quantum computers matches perfectly with imec's track record of and commitment to pushing the leading edge of integrated technologies," adds Haris Osman, VP R&D and head of department.

"Xanadu's ultimate mission is to build quantum computers that are useful and available to people everywhere. To do this we have the ambitious goal of reaching one million qubits using photonics. Working with imec will help us build the right foundation based on fault tolerance and error-correctable qubits," said Christian Weedbrook, Xanadu Founder and CEO. "One of the best parts of working with imec is their agility and ability to scale production on new platforms by transferring them to top production foundries around the world," he added.

Xanadu offers cloud access to both photonic quantum hardware and software solutions over its Xanadu Cloud platform. It recently announced a $100 million round led by Bessemer Venture Partners giving a total of $145 million raised thus far.

# 20. This ransomware has returned with new techniques to make attacks more effective

by Danny Palmer
https://www.zdnet.com/article/this-ransomware-has-returned-with-new-techniques-to-make-attacks-more-effective/

There's been a rise in cyber attacks using a form of ransomware that first appeared almost two years ago. But despite being relatively old, it's still proving successful for cyber criminals.

Cybersecurity researchers at Trend Micro have detailed an increase in LockBit ransomware campaigns since the start of July. This ransomware-as-a-service first appeared in September 2019 and has been relatively successful, but has seen a surge in activity this summer.

In adverts on underground forums, LockBit's authors claim that LockBit 2.0 is one of the fastest file-encrypting ransomware variants in the market today. And those claims have proven interesting to cyber criminals seeking to make money from ransomware.

Trend Micro researchers have seen a number of LockBit ransomware campaigns in recent weeks, predominantly targeting organisations in Chile, but also the UK, Italy and Taiwan.

While LockBit has remained under the radar for much of this year, it hit the headlines with an attack against professional services firm Accenture. LockBit also appears to have benefited from the apparent disappearance of ransomware gangs including REvil and Darkside, with a significant number of affiliates of those operators turning towards LockBit as their new means of performing ransomware attacks.

The attackers often gain entry to networks using compromised Remote Desktop Protocol (RDP) or VPN accounts which have been leaked or stolen; alternatively, LockBit attacks sometimes attempt to recruit insiders to help gain access through legitimate login credentials.

LockBit has also gained success by following in the footsteps of prominent ransomware groups using certain tactics, techniques and procedures (TTPs) during attacks. For example, LockBit now uses Ryuk's Wake-on-LAN feature, sending packets to wake offline devices in order to help move laterally around networks and compromise as many machines as possible.

LockBit also uses a tool previously deployed by Egregor ransomware, using printers on the network to print out ransom notes.

"They were heavily influenced by the Maze ransomware gang and when they shut down, they appear to have shifted their focus to Ryuk and Egregor ransomware gangs TTPs," Jon Clay, VP of threat intelligence at Trend Micro, told ZDNet.

"What we can take away from this is many malicious actor gangs likely follow the news of how successful other gangs are and look to model their TTPs themselves. Ransomware has evolved over time in order to continue to be successful for its creators," he added.

Like many of the most disruptive ransomware variants, LockBit also adds a double extortion element to attacks, stealing data from the victim and threatening to leak it if the ransom isn't paid within a set period.

"The LockBit gang has been around for a while now and continue to update their TTPs in order to have successful attack campaigns," said Clay.

It's expected that LockBit ransomware attacks will continue to be a cybersecurity threat for some time, particularly given that the group is actively advertising for additional affiliates. But while ransomware groups are aggressively persistent, there are actions which information security teams can take to help protect networks from attack.

This includes applying the latest security patches and updates to operating systems and software, so cyber criminals can't exploit known vulnerabilities to help launch attacks. Organisations should also apply multi-factor authentication across the network, making it harder for cyber criminals to use stolen credentials to help facilitate attacks.

# 21. Practical Considerations for Post-Quantum Cryptography Deployment

by Massimiliano Pala
https://www.cablelabs.com/gridmetrics-launches-the-power-event-notification-system-and-its-just-the-beginning

It’s the year 2031, and the pandemic is in the past. While Dave drinks his morning coffee and reads the news, a headline catches his attention. A large quantum computer is finally operational! Suddenly, Dave’s mind is racing. After few seconds, as his heartbeat slows, he looks up into the mirror and proudly says, “Yes, we’re ready.”

What you don’t know about Dave is that he’s been working for the past 10 years to make sure that all aspects of our broadband communications and access networks remain secure and protected. Besides searching for new quantum-

resistant algorithms, Dave has been focusing on the practical aspects of their deployment and addressing their impact on the broadband industry.

Here in 2021, the broadband industry needs to start traveling the same path that Dave will have navigated 10 years from now. We need to make sure we remove the roadblocks ahead of time so that we can lay the groundwork for the adoption of new security tools like post-quantum (PQ) cryptography.

## The Post-Quantum Cryptography Landscape

Although NIST is still finalizing its standardization process for PQ cryptography, there are interesting trends and practical long-term considerations for PQ deployment and the broadband industry that we can already infer.

Most of the algorithms that are still present in the final round of the algorithm competition are based on mathematical constructs called *lattices*, which, in practice, are collections of equally spaced vectors or points. Lattice-based cryptography security properties are rooted in the difficulty of solving certain topological problems for which there is not an efficient algorithm (even for a quantum computer), such as the Shortest Vector Problem (SVP) or the Closest Vector Problem (CVP). Algorithms like Falcon or Dilithium are based on lattices and produce the smallest authentication traces overall (i.e., signatures range from 700 bytes to 3,300 bytes).

Another class of algorithms to keep an eye on is based on *isogenies*. These algorithms use a different structure than lattices and have been proposed for key exchange algorithms. These new key-exchange algorithms—namely Key Encapsulation Mechanism (KEM)—leverage morphisms (or isogenies) among elliptic curves to provide "Diffie-Hellman–like" key exchange properties to implement Perfect Forward Secrecy. Isogeny-based encryption uses the shortest keys in the PQ algorithm landscape but is computationally very heavy.

Besides these two classes of algorithms, we should keep hash-based signature schemes in mind as a possible alternative. Specifically, they provide proven security at the expense of very large cryptographic signatures (public keys are extremely small) that hinder, at the moment, their adoption. A well-known hash-based algorithm that will probably be re-included in the NIST standardization process is SPHINCS+.

## DOCSIS® Protocol, DOCSIS PKI and PQ Deployment

Now that you understand the available options to consider for your next-generation crypto infrastructure, it's time to look at how these new algorithms impact the broadband environment. In fact, although the DOCSIS protocol has been using digital certificates and public-key cryptography since its inception, the broadband ecosystem relies on the RSA algorithm only—and that algorithm has very different characteristics than the PQ algorithms in consideration today.

The good news is that from a security perspective, minimal upgrades are required to replace the use of RSA using the latest version of the DOCSIS protocol (i.e., DOCSIS 4.0) when compared with previous versions. Specifically, DOCSIS 4.0 removes the dependency on the use of the RSA algorithm in terms of key exchange and leverages a standard signature format—namely, the Cryptographic Message Syntax (CMS)—to deliver signatures. CMS is already scheduled to be upgraded to provide standard support for PQ algorithms as soon as the algorithms standardization process ends. In DOCSIS 1.0–3.1, because of the dependency on the RSA algorithm for key exchange, the required protocol changes might be more extensive and employ the use of symmetric keys, in addition to RSA keys, to deliver secure authentications.

The size of the new algorithms is another important aspect of deployment. Although the lattice-based and isogenies-based algorithms are quite efficient for the sizes of authenticated (signature) or encrypted (key-exchange) data, they're still an order of magnitude (or more) larger than what we're used to today.

Therefore, the broadband industry needs to focus a first set of considerations surrounding the impact of cryptography on the size of authentication and authorization messages. In the DOCSIS protocol, the Baseline Privacy Key Management (BPKM) messages are used, at layer 2, to transfer authentication information across the cable modem and its termination system. Fortunately, because BPKM messages can provide support for any data size via fragmentation support, we don't envision the need to update or modify the structure of Layer 2 authentication messages to accommodate the new size of crypto.

Somewhat connected to the size of the new crypto are the considerations related to algorithm performances. PQ algorithms, unlike RSA and ECDSA, are computationally very heavy and therefore might pose additional engineering hurdles when designing the hardware to support them. For end-entity devices such as cable modems and optical network units, there are various options to consider. One option, for example, is to look at the integration of modern microcontrollers that can offload computation and provide isolated environments in which algorithms can be securely executed. Another approach is to leverage trusted execution environments already available in many edge devices ' central processing units (CPUs), without the need to update today's hardware architectures. On core devices, the added CPU load—when compared with the very fast RSA verifications—might require additional resources. This is an active area of investigation.

The final set of considerations is related to algorithm deployment models and certificate chain validation considerations. Specifically, because the current implementation paradigm for PQ algorithms required by NIST doesn't use the hash-and-sign paradigm (it directly signs the data without hashing it first), there are some important considerations to make. Although this approach removes the security dependency on the hashing algorithm, it also introduces a subtle but important performance hit; the data to be authenticated or signed (i.e., when a device is trying to authenticate to the network) must be processed directly by the algorithm. This might require large data buses to carry the data to the MCU or to transition through the trusted execution environment on the CPU. Performance bottlenecks generated by the adopted signing mechanism have already been observed, and further investigations are needed to better understand the real impact over deployments.

For example, when signing with the "hash-and-sign" paradigm, the signing part of the operation on a 1TB document or 1KB document takes the same time (because you're always signing the hash that's only a few bytes in length). In comparison, when using the new paradigm (not possible with algorithms like RSA), signing times can differ wildly depending on the size of the data you're signing. This problem is even more evident when addressing the costs associated with the generation and signing of hundreds of millions of certificates via this new approach. In other words, the new paradigm, if adopted, could potentially impact certificate providers and increase the costs associated with the signing of large quantities of certificates.

## Available Tools and Projects

Now that you know where and what to look for, how can you start learning more about—and experimenting with—these new algorithms for real-world deployment?

One of the best places to start is the Open Quantum Safe (OQS) project that aims to support the development and prototyping of quantum-resistant cryptography. The OQS project provides two main repositories (open-source and available on GitHub): the base liboqs library, which provides a C implementation of quantum-resistant cryptographic

algorithms, and a fork of the OpenSSL library that integrates liboqs and provides a prototype implementation of CableLabs 'Composite Crypto technology.

Although the OQS project is a great tool to start working with these new algorithms, the provided integration with OpenSSL doesn't support generic signing operations: a limitation that might affect the possibility to test the new algorithms in different use-cases. To address these limitations and to provide better Composite Crypto support together with an hash-and-sign implementation for PQ algorithms, CableLabs started the integration of the PQ-enabled OpenSSL code with a new PQ-enabled LibPKI (a fork from the original OpenCA's LibPKI repository) that can be used for building and testing these algorithms for all the aspects of the PKI lifecycle management, from validating the full certificate chain to generating quantum-resistant revocation information (e.g., CRLs and OCSP responses).

# 22. Sierra Nevada and General Dynamics to design updated cryptographic key loaders with network connectivity

by John Keller
https://www.militaryaerospace.com/trusted-computing/article/14208658/cryptographic-key-loaders-network-connectivity

U.S. Army trusted computing experts needed upgraded cryptographic key loaders with network connectivity to fill, transfer, issue, and manage cryptographic keys. They found their solution from Sierra Nevada Corp. in Sparks, Nev., and General Dynamics Mission Systems in Dedham, Mass.

Officials of the Army Contracting Command at Aberdeen Proving Ground, Md., awarded contracts to Sierra Nevada and General Dynamics last Tuesday for the Next Generation Load Device-Medium (NGLD-M) program.

The companies will share $744.2 million over the next 10 years to develop updated National Security Agency (NSA)-certified cryptographic key load devices, including the simple key loader, to load cryptographic keys into electronic encryption machines.

The Army Contracting Command awarded the NGLD-M contract on behalf of the Army Project Manager Tactical Radios (PM TR) at Aberdeen Proving Ground, Md.

NGLD-Medium (NGLD-M) provides the same functionality as legacy fill devices while adding network connectivity to support over-the-network-key (OTNK) distribution. The NGLD-M will meet NSA certification requirements while providing a reprogrammable crypto subcomponent for future modernization requirements.

The NGLD-M also will be able to interface with the management client (MGC), NSA's key management infrastructure (KMI), and mission planning management support systems (MPMSS).

The NGLD-M can connect to and receive key material, applications, and other cryptographic products by connecting to U.S. Department of Defense (DOD) networks and will contain standard interfaces to audio fill ports, RJ45 Ethernet ports, and standard Universal Serial Bus (USB).

Users of the NGLD-M, in addition to the Army, will be the U.S. Navy, Air Force, FBI, Department of Homeland Security (DHS), and state and local governments.

# 23. A Simple Crystal Could Finally Give Us Large-Scale Quantum Computing, Scientists Say

by JARRYD PLA & ANDREW DZURAK
https://www.sciencealert.com/this-simple-crystal-could-open-the-way-to-large-scale-quantum-computing

Vaccine and drug development, artificial intelligence, transport and logistics, climate science - these are all areas that stand to be transformed by the development of a full-scale quantum computer. And there has been explosive growth in quantum computing investment over the past decade.

Yet current quantum processors are relatively small in scale, with fewer than 100 *qubits* - the basic building blocks of a quantum computer. Bits are the smallest unit of information in computing, and the term qubits stems from "quantum bits".

While early quantum processors have been crucial for demonstrating the potential of quantum computing, realizing globally significant applications will likely require processors with upwards of a million qubits.

Our new research tackles a core problem at the heart of scaling up quantum computers: how do we go from controlling just a few qubits, to controlling millions? In research published today in *Science Advances*, we reveal a new technology that may offer a solution.
.
.
.

## The solution is 'global' control

An elegant solution to the challenge of how to deliver control signals to millions of spin qubits was proposed in the late 1990s. The idea of "global control" was simple: broadcast a single microwave control field across the entire quantum processor.

Voltage pulses can be applied locally to qubit electrodes to make the individual qubits interact with the global field (and produce superposition states).

It's much easier to generate such voltage pulses on-chip than it is to generate multiple microwave fields. The solution requires only a single control cable and removes obtrusive on-chip microwave control circuitry.

For more than two decades global control in quantum computers remained an idea. Researchers could not devise a suitable technology that could be integrated with a quantum chip and generate microwave fields at suitably low powers.

In our work we show that a component known as a dielectric resonator could finally allow this. The dielectric resonator is a small, transparent crystal which traps microwaves for a short period of time.

The trapping of microwaves, a phenomenon known as resonance, allows them to interact with the spin qubits longer and greatly reduces the power of microwaves needed to generate the control field. This was vital to operating the technology inside the refrigerator.

In our experiment, we used the dielectric resonator to generate a control field over an area that could contain up to four million qubits. The quantum chip used in this demonstration was a device with two qubits. We were able to show the microwaves produced by the crystal could flip the spin state of each one.

### The path to a full-scale quantum computer

There is still work to be done before this technology is up to the task of controlling a million qubits. For our study, we managed to flip the state of the qubits, but not yet produce arbitrary superposition states.

Experiments are ongoing to demonstrate this critical capability. We'll also need to further study the impact of the dielectric resonator on other aspects of the quantum processor.

That said, we believe these engineering challenges will ultimately be surmountable - clearing one of the greatest hurdles to realizing a large-scale spin-based quantum computer.

# 24. Quantum computers — What are the security issues

by Echo Richards
https://www.moviesonline.ca/quantum-computers-what-are-the-security-issues/

Although hardly anyone is aware of this, the encryption of the information we transmit is one of the foundations of the interaction of modern societies. We use it to connect to websites, share files, or perform banking transactions. All this is due to the fact that it is possible to exchange information securely. In cryptography, as in other areas of life related to security, you can observe the “shield” and “sword” race – one party wants to keep its secrets and the other wants to get them. This race could reach a new level in the near future with advances at the intersection of quantum physics and information theory.

### Physics and quantum technologies

Quantum mechanics is one of the most dynamically developing fields of physics – many Nobel Prizes have already been awarded for achievements in this field of knowledge. Thanks to these discoveries, for example, it is possible to create a laser. The use of Kantian mechanics may also affect other areas of human life and contribute to the creation

of new inventions. Those that will affect the current way of exchanging digital information, especially those that we want to encrypt, seem to be of particular interest.

To explain the importance of quantum computers and quantum cryptography, it is necessary to point out several findings from quantum physics. It is worth starting with the fact that the behavior and locations of particles (such as photons or electrons) are random and non-deterministic – this is the fundamental discovery of quantum mechanics – predictability and statistics have replaced the predictability of conventional mechanics. In other words, elementary particles (such as electrons moving around the nucleus of an atom) fall into what are called superpositions – it is impossible to determine their position and momentum at the same time, until they are measured in different places at the same time. However, at the moment of measurement, the superposition state collapses, so that the particle's position (but not its momentum, and vice versa) can be determined.

Another important discovery is the phenomenon known as "quantum entanglement" of particles, which means that when two objects (such as photons) interact in the past, the two objects retain a "memory" of their shared past. In other words, if the parameters are measured on one particle, the state of the other particle is known in advance, and interestingly, this effect may occur regardless of the distance between the two particles.

## Quantum computers

Classical computers for information processing use a binary system, in which the "building blocks" are bits with a numerical value 1 or 0. Using a sequence of these bits, you can write any value, for example 8 bits (the so-called byte) that allows you to write numbers From 0 to 256, as a result, it allows you to encode all characters in the Latin alphabet, Arabic numbers and special characters. On the other hand, quantum computers are a completely different new type of device. To create it, it is necessary to move away from well-known and proven solutions in the field of classical geometry in favor of trying to use the properties that reality itself possesses at the subatomic level.

In 1981, A. Richard Feynman, the American pioneer in quantum electrodynamics, formulated the principles of quantum computers. Their primary property was to use, among other things, superposition, as the principle of operation of qubits (the smallest and indivisible units of quantum information), that is, the property of particles (such as electrons, photons or atomic nuclei) that allows them to be in different places at the same time, but With a different possibility. The advantage of qubits is that they can contain more information than conventional bits (they can also be quantum entangled with each other). Their computing power is growing exponentially (with 2 qubits we can have 4 bits of information, with 4 we can have 16 bits, etc.). However, to use this potential, algorithms are needed that are able to perform operations on these overlays, and finally calculate the result (traditional computers are still needed here) – these operations are repeated many times and the result is averaged.

It should be emphasized that quantum computers (so far) can be faster at solving a limited set of problems – those that require parallel processing of data. In other words, they will not replace traditional computers, at least for the foreseeable future. However, this narrow slice where quantum computers can become much faster than conventional machines is critical to modern cryptography.

In 2019, Google declared its quantum supremacy – the fact that a 53-qubit computer was capable of computing faster than today's supercomputers. Instead of counting 10 thousand. A year, Google's computer completed the task in 200 seconds. After the fact, IBM specialists pointed out an error in the data and showed that their supercomputer would need two and a half days to complete the task. Therefore, the indisputable quantum supremacy still had to wait. So far, Google technicians have solved the problem (they generated a string of random numbers), which, while important, is not important from a security perspective – they haven't yet decrypted the encrypted message. However, there are

many indications that it is only a matter of time before the efficiently used qubits speed up factorization, i.e. decomposition into prime numbers of keys commonly used today to encrypt information. In other words, in the Coded Sword and Shield race, the Quantum Sword might gain an advantage soon. The security of most security measures in use today will then be questioned.

## "Quantum Sword"

Confidence in cryptographic algorithms currently in use is based on trust in the rules of mathematics. Nowadays, encrypting information with a 256-bit key sufficiently protects our communications against decryption – a supercomputer that would be able to perform billions of operations per second would take millions of years to decrypt. However, there is a risk that quantum computers could do such a task faster, provided they have the appropriate algorithms at their disposal. This algorithm was introduced in 1994 by Prof. Peter Shor, allows decomposing large natural numbers into primes, provided a sufficiently powerful quantum computer is used. So it seems only a matter of time before quantum computers equipped with proper algorithms become a serious national security challenge. This is due to the fact that, perhaps in a dozen years or so, the currently stolen information will be decrypted, although thanks to the use of quantum computers in the future, the secrets in it will be revealed. This fear generated the movement known as post-quantum cryptography.

## "Quantum Shield"

Diagnosing the threats arising from the development of quantum technologies has contributed to more extensive work on the "shield" – a new way of building and transmitting cryptographic mechanisms (the keys used to secure information). Significantly, these efforts also use findings from quantum physicists (including principles of randomness and quantum entanglement). Implementing quantum security will make the connection secure again, because to decrypt it, not only the laws of mathematics will have to be broken, but the laws of nature themselves. The security of quantum cryptography results, among other things, from the fact that anyone wishing to eavesdrop on the transmitted information by mere observation will alter it, which will not only distort the transmitted information, but also inform the sender and receiver of the eavesdropping. These solutions are currently used to a very limited extent by the armed forces and some financial institutions, but they will likely become a new standard for encryption and data transmission in the near future (eg within the 6G network).

The introduction of such solutions will have both positive and negative consequences. Since it is the laws of physics, and not mathematical rules, that will protect the security of transmitted information, the brand of the supplier of communication equipment will not matter. In other words, devices of any production can be used in data transmission networks – it does not matter whether the manufacturer deliberately inserted some vulnerability in the code that would allow eavesdropping, thanks to the fact that no eavesdropping in quantum cryptography can not be done disclosed.

In addition, with the first successes, work on the use of, among other things, quantum entanglement for the purposes of data exchange. In 2020, Chinese scientists were able to link quantum memories together over a distance of 50 kilometers. At the same time, it should be noted that currently secure quantum communication is possible (using photons) over short distances over optical fibers. This situation could improve because another team of scientists was recently able to transmit simple information over 600 km. This performance can be improved by placing a signal transducer in space. Then, using satellites, the signal (the entangled pairs of photons that make up the key) can be sent across the entire planet's space, and then the dream of a crack-resistant Internet can become a reality.

## Conclusions

Today, quantum computers are at a similar stage of development as the personal computers of the 1970s, and like artificial intelligence, they can perform very narrowly specialized tasks. However, it is likely, in terms of cryptography, that the race between "sword" and "shield" can certainly be decided in favor of "shield". However, you have to be patient. We still have to wait for the final effects. After the hype around quantum technology, there will certainly be a period of disappointment, but then (maybe not 10 years ago) there was a period of standardization and efficient applications that would deliver both a secure quantum internet and quantum computers under this roof.

# 25. Scientists removed major obstacles in making quantum computers a reality

by PRANJAL MEHAR
https://www.techexplorist.com/scientists-removed-major-obstacles-making-quantum-computers-reality/40634/

Quantum engineers from UNSW Sydney have removed a decades-old major hurdle: how to reliably control millions of qubits in a silicon quantum computer chip? They come up with a new method that can efficiently control millions of spin qubits.

Spin-based silicon quantum electronic circuits offer a scalable platform for quantum computation. They combine the manufacturability of semiconductor devices with the long coherence times afforded by spins in silicon. Advancing from current few-qubit devices to silicon quantum processors with upward of a million qubits, as required for fault-tolerant operation, presents several unique challenges. One of the most demanding is the ability to deliver microwave signals for large-scale qubit control.

Dr. Jarryd Pla, a faculty member in UNSW's School of Electrical Engineering and Telecommunications, said, "Up until this point, controlling electron spin qubits relied on us delivering microwave magnetic fields by putting a current through a wire right beside the qubit."

"This poses some real challenges if we want to scale up to the millions of qubits that a quantum computer will need to solve globally significant problems, such as the design of new vaccines."

"First off, the magnetic fields drop off quickly with distance, so we can only control those qubits closest to the wire. That means we would need to add more and more wires as we brought in more and more qubits, which would take up a lot of real estate on the chip."

"And since the chip must operate at cold temperatures, below -270°C, introducing more wires would generate way too much heat in the chip, interfering with the reliability of the qubits. So we come back to only being able to control a few qubits with this wiring technique."

Completely reimagine the silicon chip structure is the solution to the problem. Scientists started by removing the wire next to the qubits. They then applied a novel way to deliver microwave-frequency magnetic control fields across the entire system. This approach could provide control fields to up to four million qubits.

Scientists added their newly developed component called a crystal prism and a dielectric resonator. When microwaves are directed into the resonator, it focuses the wavelength of the microwaves down to a much smaller size.

Dr. Pla said, “The dielectric resonator shrinks the wavelength down below one millimeter, so we now have a very efficient conversion of microwave power into the magnetic field that controls the spins of all the qubits.”

“There are two key innovations here. The first is that we don’t have to put in a lot of power to get a strong driving field for the qubits, which crucially means we don’t generate much heat. The second is that the field is very uniform across the chip so that millions of qubits all experience the same level of control.”

UNSW, Scientia Professor Andrew Dzurak said, “We were overjoyed when the experiment proved successful. This problem of how to control millions of qubits had been worrying me for a long time since it was a major roadblock to building a full-scale quantum computer.”

Scientists are planning to use this technology to simplify the design of near-term silicon quantum processors.

# 26. Things to Avoid in a Press Release for Your Quantum Organization

https://quantumcomputingreport.com/things-to-avoid-in-a-press-release-for-your-quantum-organization/

We see a lot of quantum press releases here at the Quantum Computing Report and for those writing them we would like to provide a few tips that may make them more effective.

You may have noticed that we never publish press releases verbatim but rather write up concise summaries of the releases with a few additional analytical comments and then put a link at the end for anyone who wants to view the original release.

We do this because the typical QCR reader is very busy and wants to keep up with what is happening in the quantum world without wasting a lot of time. As a result, we try to keep our articles as brief as possible without missing any of the key ideas. This stems from my prior experience working for a Vice-President at Intel whose favorite word was “pithy” (Definition: Terse and full of substance or meaning). He would say “Don’t write a three page memo on something when you could communicate the same message in three sentences”!

The first thing to keep in mind that a press release is a marketing document. Usually, there are three key potential audiences that you should want to target: **Customers** you might want get, **Employees** you might want to recruit and **Investors** that you might want to attract. Trying to impress others like family, friends or the general public might make you feel good, but it probably won’t help you move your company forward.

We believe that these target audiences of customers, employees, and investors are already quite sophisticated and knowledgeable about quantum computing and its potential. Although some of the items below might have been helpful a few years ago when quantum was just starting to be commercialized, there has been so much press and publicity over the past few years that saying these things now sounds redundant and unnecessary. Based upon this, here are some things to avoid.

## What to Avoid

- **Basic explanations of what quantum computing is.** Putting in a press release something like "Classical computing relies on binary states in order to complete logical operations and that state is either on or off. In contrast, quantum computing is based on physical systems that can be in multiple states simultaneously, with each state having a probability of occurring after measurement" is not going to be anything new to the PhD student you are trying to recruit or the enterprise data researcher who has been studying quantum for the past year.

- **Broad characterizations of where quantum computing could be used.** We don't believe that repeating comments like "Quantum computing has the potential to benefit many industries, including those focused on drug development, logistics, manufacturing, finance and materials design" add value to a press release either. Again, this is something that your target audience has seen hundreds of time before and already knows.

- **Quotes from your new investors in a funding press release.** Perhaps a company will be obligated to include them because they just gave you money, but mostly they are generic and have a lot of fluff. Statements like "We are excited about the great team at company X and the progress they have been making. We anticipate their technology will lead the quantum market in years to come" are to be expected from someone who just invested in you and quickly ignored.

## What to Include

Too often, we see press release that announce new partnerships without saying much about what each partner will contribute. We know there are some partnerships which are more window dressing than actual cooperative work but we hope that your partnership is not one of them. Better explanations of how the companies will work together, what contributions will be made from each side and how the partnership will achieve synergy from the combination of the two efforts will make the announcement more meaningful.

Similarly, we see product announcements without much technical detail. Although we realize that a press release should not be a recitation of the product's data sheet, it should list a few of the strongest features of the product and then include a link to a data sheet or technical paper that is posted on the company's website. No one is going to contact you to buy the product when they don't have an idea of what it is or how good it works.

Finally, quantum companies should realize that the quantum industry is getting to be very competitive. There are hundreds of companies working in quantum and there will likely be a few of them that are doing something similar or, at least, an alternative to what you are offering. It is not enough to talk about why the quantum industry will succeed, you must show why specifically **your company** will succeed. A press release can be a key vehicle for you to differentiate your company and show what is special about your approach and why you will be a winner. Clients, employees, and investors all want to be associated with winners!

## Summary

As with many activities it is something best to approach developing a press release by first thinking about who your audience is and what result you want to achieve and then working backwards from there. A press release is a key marketing document that can help contribute to the overall success of your business. It pays to take time to craft a

press release that achieves maximum effect rather than just jotting down something in a hurry. If you end up targeting the wrong audience or leave them something that doesn't get them interested, you are wasting your time and money.

# 27. A Question Of Biggitude: Your Organization's Cryptography

by Mike Brown
https://www.forbes.com/sites/forbestechcouncil/2021/08/13/a-question-of-biggitude-your-organizations-cryptography/?utm_medium=email&_hsmi=154123099&_hsenc=p2ANqtz-_5fbOKQn7L9e--SlkglKsz6mgwLWwp_EzJmn3nPxN-SuJk8YtI3qagR2146d5Foek_78h4g8VoEddbJRbQ5MFqYCSIJA&utm_content=154123099&utm_source=hs_email&sh=69b7cb7e5c6a

How many grains of sand are there in the world? You have likely asked this at some point in your life. The enormity of that number is mind-boggling. Author David Blatner wrote about such wonders in *Spectrums: Our Mind-Boggling Universe from Infinitesimal to Infinity*. With numbers so high, Blatner says we "can't handle the biggitude."

Like the grains of sand in the world, cryptography is everywhere — and sometimes it's challenging for organizations to keep track of. It's a question of biggitude. Cryptography is at the core of every secure transaction, every safe automobile, every form of communication. Think about when you send money to a friend, check your email or make a purchase online. Our fast-moving world is dependent on encryption, a critical component of every layer of the computing architecture — hardware, operating systems, network protocols, applications — found on-premises, in the cloud, in mobile, distributed or on connected devices in the internet of things (IoT). Why is this pervasive set of technologies that we've been relying on since the 1970s, but never paid too much attention to, suddenly needing our attention?

To address security threats, minimize risks and future-proof systems, especially with cryptographic standards in flux and updates by the National Institute of Standards and Technology (NIST) about new standards coming in late 2021, it's paramount for enterprises to embrace a centralized approach to cryptographic management. Imagine how difficult it can be for enterprises to inventory their cryptography assets across entire infrastructures when much of it's hidden, outdated or housed within a third-party organization. It's a resource-heavy and time-consuming task that, by the time it's finished, generates information that's no longer fresh and requires the process to start over again.

## Implementing A Cryptographic Center Of Excellence To Help Meet Challenges

Can establishing and implementing a cryptographic center of excellence (CryptoCoE) help? As organizations prepare for incoming cryptographic transitions, prioritizing cryptographic management is a critical success factor. One of the largest cryptography transitions in history will be the one from classical to quantum-safe cryptography. The looming quantum computer threat to encryption has led some organizations to embark on implementing a CryptoCoE to mitigate cryptographic threats.

Threats to cryptography, such as quantum computing, will have a significant — even detrimental — impact on every modern business. The fact that migration takes a long time adds to the challenge, making strategic, long-term planning a must.

According to one of our global finance partners in Switzerland, one of the key issues is the lack of visibility into cryptography; you can't quantify the risk of something you're not aware of, let alone manage it. This bank has implemented a cryptographic center of excellence, which I think is a great idea since the larger an enterprise, the more difficult it is to have central governance.

Here's what's at stake: Cryptographic changes, such as public key infrastructure (PKI) migration, from classic to quantum-safe standards, are massive and disruptive in size, scope and complexity. Chief information security officers (CISOs) often have no visibility into their organization's cryptographic posture, with limits the ability to articulate the footprint and scope of the infrastructure impacted. This makes it complicated to make the case for additional resources and budget.

Similarly, IT departments often have little visibility into cryptographic configurations and the cryptography in operation across hundreds of thousands of live transactions. Getting a grasp of the cryptographic posture is often a tedious, manual effort that doesn't allow for insights into the cryptography in use. Meanwhile, organizations face incredible scrutiny to meet regulatory compliance.

## The Cryptographic Management Challenge Is Manageable

Rest assured, the cryptography management challenge, while immense, is manageable. For starters, what's required, according to the chief architect at the financial institution I mentioned, is board-level and C-level visibility and enterprise-wide oversight. Leaders need a regular, comprehensive report of the scope of the issues and threats, the impact and the solutions and path to enable sustainable, forward-moving business. Being able to migrate between the emerging crypto standards in a repeatable, manageable and cost-effective way is critical in achieving crypto-agility.

Organizations should be able to enforce cryptographic policies across all infrastructures and reign in the silos. Enterprise-wide support, including the C-suite embracing a CryptoCoE, will help get all stakeholders on board. Ultimately, this will help to answer the questions of, "What cryptography do you have in your organization?" and "What's a priority to be fixed, upgraded or replaced, and when?"

As for the question of how many grains of sand there are in the world: "If you assume a grain of sand has an average size and you calculate how many grains are in a teaspoon and then multiply by all the beaches and deserts in the world, the Earth has roughly (and we're speaking *very* roughly here) ... seven quintillion, five hundred quadrillion grains," states Robert Krulwich, science correspondent for *NPR*.

Keeping track of your cryptography can be infinitely more manageable than counting grains of sand.

# 28. A complete platform for quantum computing

by Technical University of Denmark
https://phys.org/news/2021-08-platform-quantum.html?utm_medium=email&_hsmi=154123099&_hsenc=p2ANqtz--lrXtAXOuUb-gxWzqLe8UHO4polTst9XqrtWlTzB0Kdcx2c_8iB-wXAjeZGw81XUJtI_Yk_5h3Z01DtDunO5qduBNNHVWg&utm_content=154123099&utm_source=hs_email

In a new groundbreaking work, researchers from DTU have now realized the complete platform for an optical quantum computer. The platform is universal and scalable, it all takes place at room temperature, and the technology is directly compatible with standard fiber optic networks. This puts DTU right at the forefront of the development.

Optical quantum computers have long been overshadowed by superconducting technologies that have been accelerated by huge development programs run at tech giants like IBM and Google. The situation is now changing, one reason being a string of pioneering projects performed by researchers at the basic research center bigQ at DTU Physics.

In fact, the researchers at DTU are not limiting themselves to simply developing individual components for an optical quantum computer or just a quantum simulator. They are working determinedly on developing a universal measurement-based optical quantum computer.

## Can run any arbitrary algorithm

Although the type of quantum computer that the DTU researchers are developing is conceptually very different from a normal computer, there are also similarities.

There are some basic logical devices (qubits) that carry the information, and there are gates that perform operations on one or more qubits, thus implementing an algorithm.

The demonstration of a so-called universal gate set—and the implementation of a number of operations by means thereof—is precisely what constitutes the new advance in optical quantum computing.

"Our demonstration of a universal set of gates is absolutely crucial. It means that any arbitrary algorithm can be realized on our platform given the right inputs, namely optical qubits. The computer is fully programmable," says Mikkel Vilsbøll Larsen, who has been the main driving force behind the work and who recently completed his Ph.D. studies at DTU.

## Scaling makes quantum computer practically relevant

The potential of the quantum computer is enormous, and its dramatically increased processing power relative to standard transistor-based computers will enable disruptive innovation in a wide range of areas of great importance to Denmark, such as the pharmaceutical industry, optimization of the transport sector, and development of materials for carbon capture and storage.

A crucial factor in fulfilling this potential is that the quantum computer is realized on a platform that is scalable to thousands of qubits, explains Senior Researcher Jonas S. Neergaard-Nielsen, who is one of the mainstays of the work.

"Theoretically, there's no difference between whether a quantum computer is based on superconducting or optical qubits. But there's a decisive practical difference. Superconducting quantum computers are limited to the number of qubits fabricated on the specific processor chip. In our system, we're constantly creating new ones and entangling them quantum mechanically with those we are performing calculations on. This means that our platform is easily scalable."

"In addition, we don't need to cool everything down in large cryostats. Instead, we can do it all at room temperature in optical fibers. The fact that the system is based on optical fibers also means that it can be connected directly to a future quantum Internet, without difficult intermediaries."

The researchers passed the scaling milestone already back in 2019 when they accounted for how, as some of the first in the world, they had produced the basic structure for a measurement-based optical quantum computer—a so-called two-dimensional cluster state with over 30,000 entangled light states.

## Already looking determinedly ahead

Although they might be tempted to rest on their laurels for just a while, the team of researchers already have new goals in their sight.

Earlier this year, they developed and patented a full theoretical framework for how their technology can also embrace error correction in the long term. This is one of the great current challenges for quantum computing technology.

"It's an important research result we've just published, and we're proud of it. But our ambitions go much further than that. The long-term goal is a quantum computer that can solve relevant problems and fulfil the potential we're all striving towards," says Professor Ulrik L. Andersen, who is head of bigQ and has supervised the whole research program.

"We know what it takes to place our current technology on an optical chip and introduce error correction, and we have the relevant international collaborations in place. The same applies to the corporate sector, where companies are eager to develop use cases with us."

In other words, the researchers at DTU are ready for the next challenges and to take the next step from basic research to innovation. In fact, funding is the only thing missing.

# 29. Scientists discover 'missing piece' in quantum computing breakthrough

https://news.sky.com/story/scientists-discover-missing-piece-in-quantum-computing-breakthrough-12380559

**Scientists from the University of New South Wales in Sydney, Australia, have announced the discovery of a major breakthrough in quantum computing.**

To date, quantum scientists and computer engineers have only been able to use proof-of-concept models of quantum processors that work with just a few spin qubits, the quantum equivalent of a bit.

Now, new research published in the journal Science Advances has identified a technique which the researchers claim will enable them to control millions of these qubits.

The team considers their design the "**missing jigsaw piece**" in quantum computer architecture.

In a traditional computer, a bit - the single unit of information, either a 0 or a 1 - is stored in the electronic circuit of the computer itself, specifically in the capacitor of a memory cell, with the value depending on whether the capacitor is charged or discharged.

Spin qubit quantum computers replace this capacitor with a single quantum particle - the electron - and its "spin" value.

Dr Jarryd Pla, a researcher at UNSW, explained: "Up until this point, controlling electron spin qubits relied on us delivering microwave magnetic fields by putting a current through a wire right beside the qubit.

"This poses some real challenges if we want to scale up to the millions of qubits that a quantum computer will need to solve globally significant problems, such as the design of new vaccines.

"First off, the magnetic fields drop off really quickly with distance, so we can only control those qubits closest to the wire.

"That means we would need to add more and more wires as we brought in more and more qubits, which would take up a lot of real estate on the chip."

The issue is that these chips need to operate at extremely cold temperatures, below -270C, and introducing more wires would compromise the temperature of the chip and interfere with the reliability of the qubit.

"So we come back to only being able to control a few qubits with this wire technique," Dr Pla said.

The breakthrough came in redesigning the entire structure of a chip. Instead of having thousands of control wires running across the thumbnail-sized piece of silicon, the team generated a magnetic field from above the chip which can manipulate all of the qubits simultaneously.

This had first been proposed in the 1990s, but the new research is the first practical way to achieve this.

"First we removed the wire next to the qubits and then came up with a novel way to deliver microwave-frequency magnetic control fields across the entire system. So in principle, we could deliver control fields to up to four million qubits," said Dr Pla.

The researchers then added a new component above the silicon chip, a crystal prism called a dielectric resonator, which can be used to focus the wavelength of microwaves down into a smaller size.

"The dielectric resonator shrinks the wavelength down below one millimetre, so we now have a very efficient conversion of microwave power into the magnetic field that controls the spins of all the qubits.

"There are two key innovations here. The first is that we don't have to put in a lot of power to get a strong driving field for the qubits, which crucially means we don't generate much heat. The second is that the field is very uniform across the chip, so that millions of qubits all experience the same level of control."

The team's experiments which could allow them to control millions of qubits at the same time was a success, although "there are engineering challenges to resolve before processors with a million qubits can be made", Dr Pla added.

# 30. Progress in algorithms makes small, noisy quantum computers viable

## by Los Alamos National Laboratory

https://phys.org/news/2021-08-algorithms-small-noisy-quantum-viable.html

As reported in a new article in *Nature Reviews Physics*, instead of waiting for fully mature quantum computers to emerge, Los Alamos National Laboratory and other leading institutions have developed hybrid classical/quantum algorithms to extract the most performance—and potentially quantum advantage—from today's noisy, error-prone hardware. Known as variational quantum algorithms, they use the quantum boxes to manipulate quantum systems while shifting much of the work load to classical computers to let them do what they currently do best: solve optimization problems.

"Quantum computers have the promise to outperform classical computers for certain tasks, but on currently available quantum hardware they can't run long algorithms. They have too much noise as they interact with environment, which corrupts the information being processed," said Marco Cerezo, a physicist specializing in quantum computing, quantum machine learning, and quantum information at Los Alamos and a lead author of the paper. "With variational quantum algorithms, we get the best of both worlds. We can harness the power of quantum computers for tasks that classical computers can't do easily, then use classical computers to compliment the computational power of quantum devices."

Current noisy, intermediate scale quantum computers have between 50 and 100 qubits, lose their "quantumness" quickly, and lack error correction, which requires more qubits. Since the late 1990s, however, theoreticians have been developing algorithms designed to run on an idealized large, error-correcting, fault tolerant quantum computer.

"We can't implement these algorithms yet because they give nonsense results or they require too many qubits. So people realized we needed an approach that adapts to the constraints of the hardware we have—an optimization problem," said Patrick Coles, a theoretical physicist developing algorithms at Los Alamos and the senior lead author of the paper.

"We found we could turn all the problems of interest into optimization problems, potentially with quantum advantage, meaning the quantum computer beats a classical computer at the task," Coles said. Those problems include simulations for material science and quantum chemistry, factoring numbers, big-data analysis, and virtually every application that has been proposed for quantum computers.

The algorithms are called variational because the optimization process varies the algorithm on the fly, as a kind of machine learning. It changes parameters and logic gates to minimize a cost function, which is a mathematical expression that measures how well the algorithm has performed the task. The problem is solved when the cost function reaches its lowest possible value.

In an iterative function in the variational quantum algorithm, the quantum computer estimates the cost function, then passes that result back to the classical computer. The classical computer then adjusts the input parameters and sends them to the quantum computer, which runs the optimization again.

The review article is meant to be a comprehensive introduction and pedagogical reference for researches starting on this nascent field. In it, the authors discuss all the applications for algorithms and how they work, as well as cover challenges, pitfalls, and how to address them. Finally, it looks into the future, considering the best opportunities for achieving quantum advantage on the computers that will be available in the next couple of years.

# 31. Two companies compete for US Army cryptographic key orders

by The Shephard News Team
https://www.shephardmedia.com/news/defence-notes/two-companies-compete-us-army-cryptographic-key-or/

**Sierra Nevada** and **General Dynamics Mission Systems** will compete for orders to provide the network-enabled Next Generation Load Device-Medium (NGLD-M) cryptographic key for the US Army, the DoD announced on 10 August.

The contract has an overall value of $744.22 million.

The US Army issued an RfP for NGLD-M in November 2020. A total of five bids were received, among them CACI offering its Mission Crypto Loader.

Work locations and funding will be determined with each order, with an estimated completion date of 8 August 2031.

The US Army stated when it released the RfP that the maximum requirement is for 265,000 NGLD-M units.

NGLD-M is an attempt to modernise cryptographic key load devices that are essential for joint service network security. It will replace the ageing Simple Key Loader which dates from the early 2000s.

According to the US Army, the new key will be a ruggedised, battery-powered, handheld device to manage and transfer cryptographic key material and mission planning data.

Modern cryptographic algorithms will be transferred by NGLD-M to counter the threat posed by increased proliferation of cyber and EW threats.

NGLD-M will support all command echelons across the US armed forces, other US federal government agencies and allied foreign militaries.

# 32. Best of both worlds — Combining classical and quantum systems to meet supercomputing demands

by Nagoya City University
https://www.sciencedaily.com/releases/2021/08/210812161908.htm

One of the most interesting phenomena in quantum mechanics is "quantum entanglement." This phenomenon describes how certain particles are inextricably linked, such that their states can only be described with reference to each other. This particle interaction also forms the basis of quantum computing. And this is why, in recent years, physicists have looked for techniques to generate entanglement. However, these techniques confront a number of engineering hurdles, including limitations in creating large number of "qubits" (quantum bits, the basic unit of quantum information), the need to maintain extremely low temperatures (<1 K), and the use of ultrapure materials. Surfaces or interfaces are crucial in the formation of quantum entanglement. Unfortunately, electrons confined to surfaces are prone to "decoherence," a condition in which there is no defined phase relationship between the two distinct states. Thus, to obtain stable, coherent qubits, the spin states of surface atoms (or equivalently, protons) must be determined.

Recently, a team of scientists in Japan, including Prof. Takahiro Matsumoto from Nagoya City University, Prof. Hidehiko Sugimoto from Chuo University, Dr. Takashi Ohhara from the Japan Atomic Energy Agency, and Dr. Susumu Ikeda from High Energy Accelerator Research Organization, recognized the need for stable qubits. By looking at the surface spin states, the scientists discovered an entangled pair of protons on the surface of a silicon nanocrystal.

Prof. Matsumoto, the lead scientist, outlines the significance of their study, "Proton entanglement has been previously observed in molecular hydrogen and plays an important role in a variety of scientific disciplines. However, the entangled state was found in gas or liquid phases only. Now, we have detected quantum entanglement on a solid surface, which can lay the groundwork for future quantum technologies." Their pioneering study was published in a recent issue of Physical Review B.

The scientists studied the spin states using a technique known as "inelastic neutron scattering spectroscopy" to determine the nature of surface vibrations. By modeling these surface atoms as "harmonic oscillators," they showed antisymmetry of protons. Since the protons were identical (or indistinguishable), the oscillator model restricted their possible spin states, resulting in strong entanglement. Compared to the proton entanglement in molecular hydrogen, the

entanglement harbored a massive energy difference between its states, ensuring its longevity and stability. Additionally, the scientists theoretically demonstrated a cascade transition of terahertz entangled photon pairs using the proton entanglement.

The confluence of proton qubits with contemporary silicon technology could result in an organic union of classical and quantum computing platforms, enabling a much larger number of qubits (106) than currently available (102), and ultra-fast processing for new supercomputing applications. "Quantum computers can handle intricate problems, such as integer factorization and the 'traveling salesman problem,' which are virtually impossible to solve with traditional supercomputers. This could be a game-changer in quantum computing with regard to storing, processing, and transferring data, potentially even leading to a paradigm shift in pharmaceuticals, data security, and many other areas," concludes an optimistic Prof. Matsumoto.

We could be on the verge of witnessing a technological revolution in quantum computing!

# 33. Post-Quantum Cryptography

by ARM
https://semiengineering.com/post-quantum-cryptography/

Quantum computing is increasingly seen as a threat to communications security: rapid progress towards realizing practical quantum computers has drawn attention to the long understood potential of such machines to break fundamentals of contemporary cryptographic infrastructure. While this potential is so far firmly theoretical, the cryptography community is preparing for this possibility by developing Post-Quantum Cryptography (PQC), that is, cryptography resisting the increased capabilities of quantum computers. In this white paper, we explore the background, impact, and urgency of this threat, and summarize the cryptographic schemes being evaluated. We also provide recommendations on what steps should be taken today to be prepared for the changes to come, and discuss how Arm is approaching PQC.

# 34. Quantum computers could threaten blockchain security. These new defenses might be the answer

by Daphne Leprince-Ringuet
https://www.zdnet.com/article/quantum-computers-could-threaten-blockchain-security-these-new-defenses-might-be-the-answer/

It might be only a matter of time before quantum computers crack the cryptography keys that support sensitive data and cryptocurrencies on blockchain networks. Now quantum software company Cambridge Quantum (CQ) says it has developed a "quantum-safe" method that could future-proof any blockchain by making the system invulnerable to quantum attacks.

CQ partnered with the Inter-American Development Bank (IDB) and its innovation laboratory IDB Lab, which has been actively investing in blockchain technology to support social and economic applications in Latin America and the Caribbean.

Specifically, IDB Lab has developed LACChain, a blockchain platform leveraged by more than 50 organizations in the region for use cases ranging from cross-border e-money payments to exchanging data between different countries' customs administrations.

CQ implemented a quantum-safe security layer to LACChain that has made the system secure from future quantum computers.

To do so, CQ deployed its own commercially available platform to protect against quantum threats, called IronBridge, to LACChain.

Blockchain's vulnerability to quantum computers comes from its extensive reliance on cryptography.

The technology, also called a distributed ledger, is essentially a computational system in which information is securely logged, shared and synchronized among a network of participants. The system is dynamically updated through messages called transactions, and each participant can have a verified copy of the system's current state and of its entire transaction history.

For this type of decentralized data-sharing system to work requires strict security protocols – not only to protect the information and communications in the blockchain, which are often sensitive, but also to confirm the identity of participants, for example thanks to digital signatures.

These protocols, for now, rely on classical cryptography keys, which transform information into an unreadable mush for anyone but the intended recipients. Cryptography keys are used to encrypt data – data that can in turn only be read by someone who owns the right key to decode the message.

The strength of encryption, therefore, depends on how difficult it is for a malicious actor to decode the key; and to make life harder for hackers, security protocols currently rely on algorithms such as RSA or the digital signature algorithm to generate cryptography keys that are as complex as possible. Those keys, in principle, can only be cracked by crunching through huge amounts of numbers.

This is why most current cryptography protocols are too hard to decode – at least with a classical computer. But quantum computers, which are expected to one day possess exponential compute power, could eventually crack all of the security keys that are generated by the most established classical algorithms.

Quantum computers are still an emergent technology, and they are nowhere near mature enough to reveal any secrets just yet. But scientists have already identified some quantum algorithms, namely Shor's algorithm, which have the potential to eventually break existing security protocols.

Alexander Lvovsky, professor at the department of physics at the University of Oxford, says that quantum computers, therefore, pose a threat to blockchain security processes like digital signatures.

"By using Shor's algorithm, a quantum attacker is able to calculate the private key of a user on the basis of their signed message, which is impossible to do with classical computers, and in this way, impersonate any party they want," Lvovsky tells ZDNet.

Quantum computers in the hands of a hacker could have dramatic consequences for the critical information that is currently stored. For example, hundreds of billions of dollars denominated in cryptocurrencies rely on blockchain ledgers, and the World Economic Forum estimates that 10% of GDP may be stored in blockchains by 2027.

This could one day be at risk from quantum attacks. Recent analysis by Deloitte estimates that a quarter of all bitcoins could be stolen with a quantum attack, which currently represents over $40 billion.

CQ and IDB, therefore, teamed up in an effort to deploy what is known as "post-quantum cryptography" to the blockchain – a form of cryptography that is adapted to a world in which quantum computers are no longer a thing of the future.

There are various ways to address post-quantum cryptography, but all approaches essentially consist of making cryptography keys harder to crack, even for quantum computers. To do so requires an extra dose of randomness, or entropy. A key that is generated purely randomly, indeed, is much harder to decode than one that is the product of a mathematical operation – which can be reverse-engineered by a powerful computer.

And while classical algorithms rely on mathematics, quantum computers can harness a special, non-deterministic property of quantum mechanics to generate this true randomness. CQ has leveraged this to create the IronBridge platform, which taps those quantum processes to create random numbers and make extra secure cryptography keys.

IronBridge was successfully used in LACChain to protect communications as well as to secure digital signatures. "LACChain blockchain was an ideal target for keys generated by our IronBridge platform," says Duncan Jones, head of quantum cybersecurity at CQ. "Only keys generated from certified quantum entropy can be resistant to the threat of quantum computing."

CQ deployed IronBridge as a "layer-two" service, meaning that it comes on top of the original architecture of the LACChain blockchain and could, therefore, be adapted to other systems.

Even if large-scale quantum computers are still some way off, the announcement is likely to address the concerns of blockchain users. Whether it is in five, 10 or 15 years, a quantum computer could crack the security protocols that are protecting information now – meaning that sensitive information that is currently being stored on the blockchain is still at risk from future hacking.

"The security currently used in most blockchains is vulnerable to quantum attack," Itan Barmes, quantum specialist at Deloitte, tells ZDNet. "No one knows when these attacks are going to become feasible. Estimates range between five and 30 years. On the other hand, migrating to a quantum-safe solution is also expected to take years, so ignoring the problem is taking an unnecessary risk."

Blockchain is not alone in helping to prepare for the future of cryptography. Governments around the world are also rushing to develop post-cryptography protocols, as concern mounts that information about defense and national security might one day be revealed by quantum computers.

The UK's National Cyber Security Centre has been saying for many years that reliance on classical cryptography needs to end, for example; while in the US, the National Security Agency is currently investigating a number of algorithms that could improve the resilience of cryptography keys.

# 35. Researchers Build New Bridge Connecting Quantum Error Correction Codes With Quantum Field Theory

by Matt Swayne
https://thequantumdaily.com/2021/08/11/researchers-build-new-bridge-connecting-quantum-error-correction-codes-with-quantum-field-theory/

In a new study from Skoltech and the University of Kentucky, researchers have found a new connection between quantum information and quantum field theory. This work attests to the growing role of quantum information theory across various areas of physics. The paper was published in the journal Physical Review Letters.

Quantum information plays an increasingly important role as an organizing principle connecting various branches of physics. In particular, the theory of quantum error correction, which describes how to protect and recover information in quantum computers and other complex interacting systems, has become one of the building blocks of the modern understanding of quantum gravity.

"Normally, information stored in physical systems is localized. Say, a computer file occupies a particular small area of the hard drive. By "error" we mean any unforeseen or undesired interaction which scrambles information over an extended area. In our example, pieces of the computer file would be scattered over different areas of the hard drive. Error correcting codes are mathematical protocols that allow collecting these pieces together to recover the original information. They are in heavy use in data storage and communication systems. Quantum error correcting codes play a similar role in cases when the quantum nature of the physical system is important," Anatoly Dymarsky, Associate Professor at the Skoltech Center for Energy Science and Technology (CEST), explains.

In a rather unexpected twist, scientists realized not too long ago that quantum gravity—the theory describing quantum dynamics of space and time—operates similar mathematical protocols to exchange information between different parts of space.

"The locality of information within quantum gravity remains one of the few open fundamental problems in theoretical physics. That is why the appearance of well-studied mathematical structures such as quantum error correcting codes is intriguing," Dymarsky notes.

Yet the role of codes was only understood schematically, and the explicit mechanism behind the locality of information remains elusive.

In their paper, Dymarsky and his colleague, Alfred Shapere from the University of Kentucky Department of Physics and Astronomy, establish a novel connection between quantum error correcting codes and two-dimensional conformal field theories. The latter describe interactions of quantum particles and have become standard theoretical tools to describe many different phenomena, from fundamental elementary particles to quasi-particles emerging in quantum materials, such as graphene. Some of these conformal field theories also describe quantum gravity via holographic correspondence.

"Now we have a new playground to study the role of quantum error correcting codes in the context of quantum field theory. We hope this is a first step in understanding how locality of information actually works, and what hides behind all this beautiful mathematics," Dymarsky concludes.

# 36. Riverlane awarded the first contract to supply quantum software to the UK's National Quantum Computing Centre

by Amy Flower
https://www.riverlane.com/news/2021/08/riverlane-to-supply-quantum-software-to-the-uks-national-quantum-computing-centre/

Riverlane has been awarded the first contract to supply quantum software to the UK's National Quantum Computing Centre (NQCC). The NQCC, funded through UK Research and Innovation, is dedicated to accelerating the development of quantum computing in the UK.

Quantum computing has the potential to benefit many industries, including those focused on drug development, finance and materials design. Delivering on this potential requires formidable developments in hardware and software to be able to reliably control the growing numbers of qubits necessary to power quantum computers. A key milestone on the pathway to practical quantum machines is the development of benchmarking tools that can assess qubit errors and overall system performance. Under the contract, our quantum scientists and engineers will deliver a benchmarking software suite that will allow comparison of the performance of different quantum computing resources. It will also provide significant insights into hardware architectures, latency and other factors related to the practical implementation of error correction.

Dr Steve Brierley, CEO of Riverlane, said: "We are thrilled that the NQCC recognises the incredible potential of quantum computing and are very proud to be their first supplier of quantum software. Riverlane aims to support the NQCC's role in becoming a trusted authority and provider of national capabilities in quantum computing".

Dr Michael Cuthbert, the Centre Director of NQCC, said: "I am delighted we are able to make this first contract award, following a competitive process. The NQCC aims to address the challenge of scaling emerging quantum computing technologies with the goal of delivering a 100+ qubit machine by 2025. This contract award to Riverlane is an initial step, demonstrating how we will form collaborations across industry and the research community to grow our capability. The benchmarking suite, combined with noise mitigation processes will support delivery of useful tools for the centre's technology, applications and user programmes."

# 37. Quantum computing: How BMW is getting ready for the next technology revolution

by Daphne Leprince-Ringuet
https://www.zdnet.com/article/quantum-computing-how-bmw-is-getting-ready-for-the-next-technology-revolution/

Quantum computing may still be at an early stage, but BMW has been quietly ramping up plans for the moment when it reaches maturity.

Most recently, the company just launched a "quantum computing challenge" – a call for talent designed to encourage external organizations to come up with solutions that will help the car manufacturer make the best use of quantum technologies.

"It's a search for hidden gems," Oliver Wick, technology scout at BMW Research and Technology, tells ZDNet.

"It's a clear message to the world that BMW is working on quantum, and if you have innovative algorithms or great hardware, then please come to us and we can check if we could use it for BMW."

The challenge, which is run in partnership with Amazon's quantum computing division AWS Braket, is targeting corporations as well as startups and academics with a simple pitch: come up with quantum solutions to the problems that BMW has identified.

Specifically, explains Wick, BMW wants to see four challenges addressed. In the pre-production stage, quantum algorithms could help optimize the configuration of features for the limited number of cars that can be assembled for various tests, so that as many tests as possible can be carried out with a minimal amount of resources.

Similarly, optimization algorithms could improve sensor placement on vehicles, to make sure that the final configurations of sensors can reliably detect obstacles in different driving scenarios – something that is becoming increasingly important as autonomous driving becomes more common.

Candidates have also been invited to submit ideas for the simulation of material deformation during production, to predict costly problems in advance, as well as for the use of quantum machine learning to classify imperfections, cracks and scratches during automated quality inspection.

Participants are required to submit a concept proposal for any of the four challenges, after which a panel of experts will shortlist the most promising ideas. The successful candidates will then have a few months to build out their solutions on Amazon Braket, before pitching them next December. Winning ideas will earn a contract with BMW to implement their projects in real-life pilots.

"We are using the power of the crowd to solve our own problems inside BMW," says Wick.

The quantum challenge is only the latest development in a strategy that aims to aggressively push the company's quantum readiness.

BMW's high-performance computers are currently handling 2,000 tasks a day, ranging from high-end visualizations to crash simulations; but even today's most sophisticated systems are fast reaching their computing limits.

Quantum computers, however, could one day carry out computations exponentially faster, meaning that they could resolve problems that classical computers find intractable. For example, the amount of compute power required to optimize vehicle sensor placement is proving to be increasingly challenging for classical algorithms to take on; quantum algorithms, on the other hand, could come up with solutions in minutes. At BMW's production scale, this could mean huge business value.

Wick explains that the potential of quantum computers was identified by the company as early as 2017. A tech report promptly followed to acquire some knowledge about the technology and its key providers, before work started on proofs of concept.

At this stage, says Wick, the biggest challenge was to find out the business case for quantum computing. "We initiated proofs of concept in optimization or scheduling, but those were activities in which no business case was included," says Wick. "Initially, everybody came to me asking why we even needed quantum computing."

But now proof of concepts are slowly starting to emerge as business projects. One of the company's first research proposals, for instance, looked at the use of quantum computers to calculate the optimum circuit to be followed by a robot sealing welding seams on a vehicle. More recently, BMW unveiled that it has been making progress in designing quantum algorithms for supply-chain management, which have been successfully tested on Honeywell's 10-qubit system.

BMW says it has now identified over 50 challenges at various stages of the value chain where quantum computing could provide significant benefits – four of which have now been delegated to the crowd thanks to the quantum challenge.

In other words, from a blue-sky type of endeavor, quantum computing is now solidly implanted in BMW's strategy. "We've now built two teams, one in the development department and one in the IT department," says Wick. "From this perspective, we have integrated quantum computer in our strategy."

Partnerships are central to this approach. Last June, BMW co-founded the Quantum Technology and Application Consortium (QUTAC), together with firms ranging from Bosch to Volkswagen. The objective, says Wick, is to come up with a set of problems shared across different industries, to join forces in finding solutions that can then be applied to each specific use case.

BMW is also providing a €5.1 million ($6 million) to the University of Munich to support a professorship, who will be expected to conduct research into applying quantum technologies to industry problems such as those faced by BMW.

But just because quantum computing has become part of BMW's business strategy doesn't mean that the technology is already generating value. Quantum computers are still small-scale experimental devices that are utterly incapable of running programs large enough to be useful. They are known as Noisy, Intermediate-Scale Quantum Computers (NISQ), a term of reflective of how emergent the technology remains.

"We are in the NISQ era and we will need better quantum computers," says Wick. "Personally, I think we could start having business benefits in five years. But that doesn't mean we should wait for five years, lay back, and let other companies do the work instead."

Preparing for large-scale quantum computers means developing partnerships with the best talent, filing patents to secure IP, but also understanding company processes very well to know how to reform them.

"You need imagination to re-think your own processes," says Wick. "I can imagine that in the next 20 years, BMW customers will sit in front of a screen and configure their own BMW in real time, for example. This is what quantum computing is for – to re-think processes and setups."

The biggest challenge for now, according to Wick, is to fully understand the ever-expanding quantum ecosystem, to make sure that the right quantum algorithms are fitted with the right quantum hardware to solve the right company problem.

This is easier said than done in a field that is buzzing with activity, and where noise and reality can be hard to distinguish. Quantum computing is rapidly joining blockchain, AR, VR and others on the list of popular buzzwords, and Wick can only count on his experience as a technology scout to make sure that the company doesn't fall to the quantum hype.

In the automotive industry, BMW's competitors are getting ready for quantum computing to change business processes, too. Volkswagen, for one, was early in joining the bandwagon, and has been expanding its capabilities ever since. The pressure is on to not fall behind in the race for quantum technologies, or so it would seem – and BMW is making it clear that it wants to be in the lead.

# 38. Microsoft announces new ransomware detection features for Azure

by Jonathan Greig

https://www.zdnet.com/article/microsoft-announces-new-ransomware-detection-features-for-azure/

Microsoft has unveiled a new ransomware detection feature for its Azure customers that will send alerts to security teams when the system observes actions "potentially associated with ransomware activities."

Microsoft's Sylvie Liu said Azure worked with the Microsoft Threat Intelligence Center to create Fusion detection for ransomware in a blog post. Microsoft's Fusion technology uses machine learning to find potential attacks in progress and alert security teams.

The system will send alerts when it sees ransomware activities at "defense evasion and execution stages during a specific timeframe."

Liu explained that the system would send messages like "Multiple alerts possibly related to Ransomware activity detected" in the Azure Sentinel workspace.

The alerts will explain what happened and on which devices or hosts the actions were seen. The Fusion system will correlate data from Azure Defender (Azure Security Center), Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Cloud App Security and Azure Sentinel scheduled analytics rules.

A report from cybersecurity firm BlackFog released on Monday found that ransomware attacks on government organizations and schools are continuing to increase in 2021, both of which deploy thousands of Microsoft machines.

Liu cited a report from PurpleSec that estimated ransomware attacks in 2020 caused $20 billion worth of damage and increased downtime by 200%.

"Preventing such attacks in the first place would be the ideal solution, but with the new trend of 'ransomware as a service' and human-operated ransomware, the scope and the sophistication of attacks are increasing -- attackers are using slow and stealth techniques to compromise the network, which makes it harder to detect them in the first place," Liu said.

"When it comes to ransomware attacks, time more than anything else is the most important factor in preventing more machines or the entire network from getting compromised. The sooner such alerts are raised to security analysts with the details on various attacker activities, the faster the ransomware attacks can be contained and remediated."

In July, Microsoft's 365 Defender Research Team revealed three vulnerabilities in Netgear routers that could have led to data leaks of a full system compromise. The vulnerabilities were patched earlier this year.

# 39. The Quantum Internet Space Race Is Accelerating

by Jim Ricotta
https://thequantumdaily.com/2021/08/10/the-quantum-internet-space-race-is-accelerating/

In early June, when researchers from Spain and China simultaneously published two independent breakthroughs towards the development of quantum repeaters, it may have seemed like a surprising coincidence. On the contrary, these two experiments mark just the latest in an accelerating global race towards a quantum internet.

## What exactly is the quantum internet?

### Entanglement: The fundamental resource of the quantum internet

Where the classical internet transmits bits from sender to receiver, the quantum internet distributes entanglement. Entanglement is the quantum phenomenon where quantum bits — or qubits — can become intertwined across long distances. *The ability to distribute quantum Entanglement as a Service (EaaS) is at the core of the quantum internet.*

While there isn't a direct analogy to classical networks, EaaS represents the fundamental service provided by quantum networks (QNs) in the same way that TCP/IP defined the core service provided by today's internet. EaaS connects quantum network users with entangled qubits across long distances using networks of quantum repeaters.

With EaaS, applications running on nodes connected to the quantum internet will be able to request entanglement on demand. EaaS networks establish entanglement by distributing pairs of entangled photons between nodes. Once established, entanglement allows for communication exchange without the need for physical transmission.

## Why do we need the quantum internet?

**Realizing the promise of unhackable communications**

This ability to convey information on an EaaS network — without physical transmission — makes quantum networks "unhackable." Traditional threats, like eavesdropping or "man-in-the-middle" attacks are rendered impossible by the fundamental laws of physics. As we build ever more powerful quantum computers, data transmitted today, even if encrypted, could become hackable at some future date. The solution is to develop a long-term, quantum-safe security fabric such as EaaS networks.

It is critical to note that EaaS networks go beyond existing Quantum Key Distribution (QKD) networks. Today's QKD networks are single purpose, engineered specifically to support the distribution of quantum keys. EaaS networks provide entanglement as a resource, which can be used by a variety of applications. In addition, EaaS networks use teleportation to transmit qubits, providing an additional layer of security. Finally, EaaS networks support more general topologies and greater distances than QKD networks without compromising security. To support long-distance communications, QKD networks rely on trusted nodes, which can compromise security if the network is managed by a third party, such as a service provider. EaaS networks use quantum repeaters to establish direct entanglement, meaning that the network user does not need to trust the network provider.

**High Performance Computing Through Networked Quantum Computers**

EaaS enables scalable *distributed* quantum computing by networking together many small quantum computers to address larger problems. Networking quantum computers using EaaS can, for example, turn 10 50-qubit quantum computers into one 500-qubit machine. In this way, the quantum internet will drive a revolution in high performance computing (HPC), with the potential to enable breakthroughs in AI, medicine, materials, logistics, and much more.

## Why are quantum repeaters important to the quantum internet?

**Quantum repeaters: The building blocks**

To distribute EaaS across the globe in a quantum internet, we need practical quantum repeaters. In a classical network, bits are transferred along fiber optic cables, and over long distances begin to lose reliability as the signal is absorbed. Repeaters are inserted between nodes to measure the signal coming in from one side, copy it, and retransmit it at a higher power to the other side – so we can reliably transmit information over very long distances. While loss is also a problem in quantum networks, it can't be solved in the same way thanks

to physics – quantum information cannot be copied without being destroyed, a fact known as the no-cloning theorem.

Quantum repeaters are based on the concept of entanglement swapping – using teleportation to create long-distance entanglement through a chain of locally-connected repeaters. Quantum repeaters convert a series of short-range entanglements into a single long-range connection.

## What is ‘breakthrough ’about the recent quantum repeater research?

**Practical quantum repeaters**

Quantum repeater development made a leap forward in June, when two groups of researchers made independent advances towards practical quantum repeaters. So far, practical quantum repeaters have proved elusive. In the recent publications, the two groups of researchers demonstrated novel platforms for quantum repeaters that could lead to practical applications.

Simply producing entanglement is not enough. Quantum repeaters need to do so at high rates, in a way compatible with existing telecom infrastructure, and with long qubit storage times. With the two recent advancements, the field has taken a step closer towards practical quantum repeaters, which in turn hold the key to the quantum internet.

## A global race

These two developments are only the latest in an accelerating timeline of progress towards the quantum internet. Technologically the pace has been rapid. 2020 saw a number of advances: Chinese researchers demonstrated a 1000km secure quantum network using satellites; major quantum computing companies, including IonQ and Rigetti announced plans to network their devices; Dutch researchers demonstrated a multi-node network using entanglement swapping, and, most recently, Toshiba demonstrated a secure quantum link over 600km of optical fiber.

Some of the heightened interest has been driven by governments racing to be the first to develop the technology for the quantum internet. The Innovation & Competition Act, the massive $250 billion research funding bill that was recently passed in the U.S. Senate and includes funding for quantum technology, explicitly seeks to outpace China in the development of frontier technologies like the quantum internet. Governments around the world have approached quantum internet development with a similar urgency.

The race to build a quantum internet is reaching a focal point now because the technology is reaching a level of readiness for the first quantum networks to be deployed. The promise of applications like unhackable communications and scalable quantum computing is attracting high interest from governments and commercial entities alike.

There is a lot of work left to be done, but the quantum networking field is developing more quickly than any new technology I have witnessed in my 30-year career.

# 40. A Critical Random Number Generator Flaw Affects Billions of IOT Devices

by Ravie Lakshmanan
https://thehackernews.com/2021/08/a-critical-random-number-generator-flaw.html

A critical vulnerability has been disclosed in hardware random number generators used in billions of Internet of Things (IoT) devices whereby it fails to properly generate random numbers, thus undermining their security and putting them at risk of attacks.

"It turns out that these 'randomly' chosen numbers aren't always as random as you'd like when it comes to IoT devices," Bishop Fox researchers Dan Petro and Allan Cecil said in an analysis published last week. "In fact, in many cases, devices are choosing encryption keys of 0 or worse. This can lead to a catastrophic collapse of security for any up-stream use."

Random number generation (RNG) is a crucial process that undergirds several cryptographic applications, including key generation, nonces, and salting. On traditional operating systems, it's derived from a cryptographically secure pseudorandom number generator (CSPRNG) that uses entropy obtained from a high-quality seed source.

When it comes to IoT devices, this is supplied from a system-on-a-chip (SoC) that houses a dedicated hardware RNG peripheral called a true random number generator (TRNG) that's used to capture randomness from physical processes or phenomena.

Stating that the manner in which the peripheral is being current invoked was incorrect, the researchers noted the lack of checks for error code responses across the board, leading to a scenario where the random number generated isn't simply random, and worse, predictable, resulting in partial entropy, uninitialized memory, and even crypto keys containing plain zeros.

"The HAL function to the RNG peripheral can fail for a variety of reasons, but by far the most common (and exploitable) is that the device has run out of entropy," the researchers noted. "Hardware RNG peripherals pull entropy out of the universe through a variety of means (such as analog sensors or EMF readings) but don't have it in infinite supply.

"They're only capable of producing so many random bits per second. If you try calling the RNG HAL function when it doesn't have any random numbers to give you, it will fail and return an error code. Thus, if the device tries to get too many random numbers too quickly, the calls will begin to fail."

The problem is unique to the IoT landscape as they lack an operating system that typically comes with a randomness API (e.g., "/dev/random" in Unix-like OSes or BCryptGenRandom in Windows), with the researchers highlighting the benefits of a larger entropy pool associated with a CSPRNG subsystem, thus removing "any single points of failure among the entropy sources."

Although the issues can be remediated with software updates, the ideal solution would be for IoT device manufacturers and developers to include a CSPRNG API that's seeded from a set of diverse entropy sources and ensure the code doesn't ignore error conditions, or fail to block calls to the RNG when no more entropy is available.

"One of the hard parts about this vulnerability is that it's not a simple case of 'you zigged where you should have zagged' that can be patched easily," the researchers said, stressing the need for implementing CSPRNG in an IoT operating system. "In order to remediate this issue, a substantial and complex feature has to be engineered into the IoT device."

# 41. Scientists Just Simulated Quantum Technology on Classical Computing Hardware

by MIKE MCRAE
https://www.sciencealert.com/quantum-circuits-simulated-on-classical-computers-test-the-limits-of-future-technology

Lurking in the background of the quest for true quantum supremacy hangs an awkward possibility – hyper-fast number crunching tasks based on quantum trickery might just be a load of hype.

Now, a pair of physicists from École Polytechnique Fédérale de Lausanne (EPFL) in Switzerland and Columbia University in the US have come up with a better way to judge the potential of near-term quantum devices – by simulating the quantum mechanics they rely upon on more traditional hardware.

Their study made use of a neural network developed by EPFL's Giuseppe Carleo and his colleague Matthias Troyer back in 2016, using machine learning to come up with an approximation of a quantum system tasked with running a specific process.

Known as the Quantum Approximate Optimization Algorithm (QAOA), the process identifies optimal solutions to a problem on energy states from a list of possibilities, solutions that should produce the fewest errors when applied.

"There is a lot of interest in understanding what problems can be solved efficiently by a quantum computer, and QAOA is one of the more prominent candidates," says Carleo.

The QAOA simulation developed by Carleo and Matija Medvidović, a graduate student from Columbia University, mimicked a 54 qubit device – sizeable, but well in line with the latest achievements in quantum tech.

While it was an approximation of how the algorithm would run on an actual quantum computer, it did a good enough job to serve as the real deal.

Time will tell if physicists of the future will be quickly crunching out ground states in an afternoon of QAOA calculations on a bona fide machine, or take their time using tried-and-true binary code.

Engineers are still making incredible headway in harnessing the spinning wheel of probability trapped in quantum boxes. Whether current innovations will ever be enough to overcome the biggest hurdles in this generation's attempt at quantum technology is the pressing question.

At the core of every quantum processor are units of calculation called qubits. Each represents a wave of probability, one without a single defined state but is robustly captured by a relatively straight-forward equation.

Link together enough qubits – what's known as entanglement – and that equation becomes increasingly more complex.

As the linked qubits rise in number, from dozens to scores to thousands, the kinds of calculations its waves can represent will leave anything we can manage using classical bits of binary code in the dust.

But the whole process is like weaving a lace rug from spiderweb: Every wave is a breath away from entangling with its environment, resulting in catastrophic errors. While we can reduce the risk of such mistakes, there's no easy way right now to eliminate them altogether.

However, we might be able to live with the errors if there's a simple way to compensate for them. For now, the anticipated quantum speedup risks being a mirage physicists are desperately chasing.

"But the barrier of 'quantum speedup' is all but rigid and it is being continuously reshaped by new research, also thanks to the progress in the development of more efficient classical algorithms," says Carleo.

As tempting as it might be to use simulations as a way to argue classical computing retains an advantage over quantum machines, Carleo and Medvidović insist the approximation's ultimate benefit is to establish benchmarks in what could be achieved in the current era of newly emerging, imperfect quantum technologies.

Beyond that, who knows? Quantum technology is already enough of a gamble. So far, it's one that seems to be paying off nicely.

This research was published in *Nature Quantum Information*.

# 42. IBM's Quantum Computing Compromise—a Road to Scale

## by EDD GENT

## https://spectrum.ieee.org/ibm-s-quantum-computing-compromise-the-road-to-scale

Quantum computers are some of the most fiendishly complex machines humans have ever built. But exactly how complex you make them has significant impacts on their performance and scalability. Industry leaders, perhaps not surprisingly, sometimes take very different approaches.

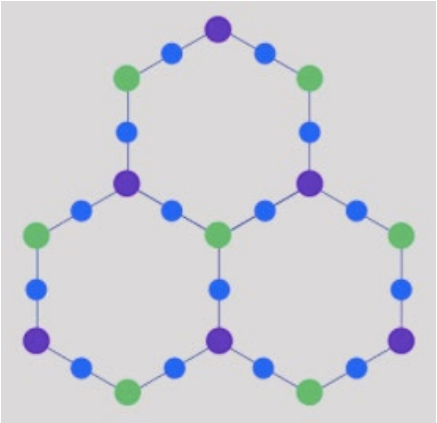
Consider IBM. As of this week (8 August), all of Big Blue's quantum processors will use a hexagonal layout that features considerably fewer connections between qubits—the quantum equivalent of bits—than the square layout used in its earlier designs and by competitors Google and Rigetti Computing.

This is the culmination of several years of experimentation with different processor topologies, which describe a device's physical layout and the connections between its qubits. The company's machines have seen a steady decline in the number of connections despite the fact its own measure of progress, which it dubs "quantum volume", gives significant weight to high connectivity.

That's because connectivity comes at a cost, says IBM researcher Paul Nation. Today's quantum processors are error-prone, and the more connections between qubits, the worse the problem gets. Scaling back that connectivity resulted

in an exponential reduction in errors, says Nation, which the company thinks will help them scale faster to the much larger processors that will be required to solve real-world problems.



Three unit cells of the so-called "heavy-hex" lattice. Colors indicate the pattern of three distinct frequencies for control (dark blue) and two sets of target qubits (green and purple).

"In the short term it's painful," says Nation. "But the thinking is not what is best today, it's what is best for tomorrow."

IBM first introduced the so-called "heavy-hex" topology last year, and the company has been gradually retiring processors with alternative layouts. After this week, all of the more than 20 processors available on the IBM Cloud will rely on the design. And Nation says heavy hex will be used in all devices outlined in its quantum roadmap, at least up until the 1,121-qubit Condor processor planned for 2023.

The basic building block is 12 qubits arranged in a hexagon, with a qubit on each point and another on each flat edge. The qubits along the edges only connect to their two closest neighbours, while the ones on the points can connect to a third qubit, which makes it possible to tile hexagons alongside each other to build larger processors.

The layout represents a significant reduction in connections from the square lattice used in the company's earlier processors—as well as most other quantum computers that rely on superconducting qubits. In that topology qubits typically connect to four neighbours to create a grid of squares. Quantum computers that use trapped-ion qubits like those made by Honeywell and IonQ go even further and permit interactions between any two qubits, though the technology comes with its own set of challenges.

The decision was driven by the kind of qubits that IBM uses, says Nation. The qubits used by companies like Google and Rigetti can be tuned to respond to different microwave frequencies, but IBM's are fixed at fabrication. This makes them easier to build and reduces control system complexity, says Nation. But the layout also makes it harder to avoid frequency clashes when controlling multiple qubits at once. Also, connections can never be completely turned off—so qubits still exert a weak influence on their neighbours even when not involved in an operation.

Both phenomena can throw calculations off, but by shifting to a topology with fewer connections, IBM researchers were able to significantly reduce both effects, which led to an exponential decline in errors.

Less connectivity makes implementing circuits considerably harder, says Franco Nori, chief scientist at the Theoretical Quantum Physics Laboratory at the Riken research institute in Japan. If two qubits aren't directly linked, getting them to interact involves a series of swap operations that pass their values from qubit to qubit until they are next to each other. The fewer direct connections, the more operations required, and because each is susceptible to errors, the process can become like a game of "telephone," says Nori.

"You whisper the information to your neighbor, but by the time it gets to the other side, the probability of it being crap is huge," he says. "You don't want to have many intermediaries."

The reduced connectivity does push up the number of operations required, says Nation. But the team found the overhead remains constant as devices scale up. If they keep up the exponential reduction in errors for each operation, its impact will quickly diminish, he adds. "You pay a price," he says. "But if you can continue to improve your two-qubit performance, over time you will more than make up for that cost."

Whether exponential reductions in error will continue is unclear. Nation admits much of the gains came from the reduction in connectivity, an avenue that has now been saturated. Further progress will need to come from advances in other areas like material sciences and hardware design.

The trade-off IBM has made makes sense though, says Fred Chong, a professor at the University of Chicago, who studies quantum computing. While Google's tuneable qubits can support more connections, they are also more complicated to build, he says. Which makes scaling them up harder. Google didn't respond to an interview request.

# 43. Vision of a Quantum Future

## by Rupesh
## https://thequantumdaily.com/2021/08/06/guest-post-vision-of-a-quantum-future/

It was early 2016 and snow was falling gently as I made my way on foot from Oxford Railway Station towards the Science Campus, home to the Clarendon Laboratory and one of the top Physics departments in the world.

I was smartly dressed for an interview to join the 'User Engagement 'team at a new and ambitious initiative for a "Quantum Computing Technology Hub" called "NQIT" (Networked Quantum Information Technologies).

In the Autumn Statement of 2013, the Chancellor of the Exchequer announced £270M funding for the UK National Quantum Technologies Programme (NQTP) – one of the first of its kind in the world.

The NQTP was designed to be cohesive, co-ordinated and commercial from the get-go; establishing four key focus areas (quantum technology hubs) with £120M public investment. These were in imaging, sensing & metrology, communications and computing; and later hubs for skills and training.

In a consortium formed of 9 universities led by Oxford, and the support of around 30 industry partners, NQIT's goal was to develop a quantum computer "demonstrator" dubbed the "Q20:20" – an aspirational 20-qubit prototype to be created by 2020 (spoiler – that didn't happen but many exciting things did, including the foundational work necessary for a new quantum industry).

*But I'm getting ahead of myself!* I checked my email as the interview location had been changed to the Denys Wilkinson Building on Keble Road. I certainly wasn't expecting the looming and ugly concrete construction from the 1960s, and thought there had been some mistake!

I was interviewed by a panel of four accomplished individuals: Professor Ian Walmsley (NQIT Director and then Pro-Vice Chancellor for Innovation and Research), Professor Dominic O'Brien (co-Director for Engineering), Tim Cook (co-Director for User Engagement, not the Apple CEO, but a self-made businessman and former Managing Director of Oxford University Innovation), and Kirsty Allen (the NQIT Hub Manager who had studied Classics at Oxford).

The leadership team were looking for a candidate with a mix of expertise: a PhD in Physics (to comfortably engage with scientists), substantial start-up experience (to engage with industry), and who could comfortably sit at the intersection of research, business and technology. That was me in a nutshell and they must have been convinced too for I got the job!

Rather than view NQIT as just a technology development project, I approached it as a start-up. During my interview I had sought a mission statement and Professor Walmsley had answered: "to be a trusted source of quantum computing". Now I amended that to be "a globally trusted source of quantum computing". The word "global" was essential to convey the ambition for the UK to lead and prosper on the world stage.

But what was the vision? Nobel Laureate, Richard Feynman, first proposed a quantum computer in 1981 – to harness nature to understand nature – nature being quantum mechanical in essence. Since that time quantum computers were more science fiction than science fact, and qubit-devices remained laboratory experiments with scientists trying to piece together a complex and delicate jigsaw puzzle.

In early 2016, quantum computers were still a gamble and a risky one. Faced with this deep uncertainty, but knowing that the **future belongs to the bold**, I crafted my own vision of what a quantum future could look like. If the current stage of development was akin to an 'acorn', I dared to imagine the 'mighty oak 'era of quantum technologies. So take a journey with me to my vision of the future. As you read this, you've faded into and become history!

Imagine a small child studying the late 20th or early 21st century in a history class. The child is perplexed and noticing, the teacher asks what is the matter. The child sighs and replies: "I don't understand. What's cancer? What's Alzheimer's? What's Parkinson's or diabetes? Why didn't people breathe clean air? Why wasn't energy free? How come people starved despite there being enough food?"

The child is horrified that medicine was not personalised to a person's DNA, horrified by the environmental damage and acts of violence. The child wonders how humanity survived these barbaric times?

The questioning child lives in a "quantum city", with powerful quantum networks effortlessly co-ordinating all manner of traffic, as well as real-time monitoring of the city's 'health'. There are cities like this all over the world and off-world too – as humanity has expanded towards the stars.

In 2016, the question for me was simple: how do we get from here to there? At the start it seemed like a ‘mission impossible ’as so many components had to come together – including government, science, technology, investment, innovation, entrepreneurship, supply chain, skills & training, media and the public.

I’ve been doing the impossible for 5 years now! The road is built brick-by-brick, engagement by engagement; slowly at first, but as the ecosystem develops, the momentum increases and the pace quickens.

The UK NQTP is now a ten year programme (until 2024), with total investment over £1B. There is a vibrant quantum landscape and growing quantum economy. Other countries are making great strides in their quantum programmes too. So it’s important that the UK retains its momentum, ambition and is willing to take risks.

I don’t know what the future holds but my hope is one where humanity comes together in peace, develop a greater understanding of the universe, and continuing the pursuit of scientific and technological advances that would seem science fiction or magical to us in the present moment.

Welcome to the quantum era and a brave new world!

# 44. Strong Encryption Is 'Absolutely Fundamental,' US Cybersecurity Chief Says

by Max Eddy
https://in.pcmag.com/security/144151/strong-encryption-is-absolutely-fundamental-us-cybersecurity-chief-says

Encryption technology sometimes seems at odds with the goals of government and law enforcement, but Jen Easterly, the recently confirmed director of the Cybersecurity and Infrastructure Security Agency (CISA), gave it her stamp of approval during today's Black Hat security conference.

The remarks came after a pre-recorded keynote address, where Easterly called for closer collaboration between government and security professionals. She then joined Black Hat and DefCon Founder Jeff Moss via remote video for a brief Q&A session, during which he asked Easterly where she stood on the issue of encryption.

Moss used the term "going dark," which is how some in government and law enforcement characterize end-to-end encryption because it cuts off their ability to see personal communications. He argued that there's a "false dichotomy" between security and privacy.

Easterly said she recognized that the issue is "hugely important" to both the Black Hat audience and the world at large. "We have to have strong encryption in order to defend [...] our networks," she said, to applause from the live audience."I realize there are other points of view across the government, but I think strong encryption is absolutely fundamental," she added.

Industry and researchers have generally resisted government efforts to weaken encryption or create so-called "backdoors" that would allow encrypted data to be read. This conflict culminated in the so-called Crypto Wars of the 1990s.

## CISA Wants You

While Easterly's comments earned her praise, the bulk of her keynote served to introduce herself and issue a call to action. She described her childhood love of Rubik's Cubes and her long history of public service in various roles, including with the US Army and the NSA.

Easterly's main topic was soliciting support from the security industry to help defend against cyberattacks on a national scale. Now is "an incredible moment in time when we have an administration that has made cybersecurity a national security imperative," particularly the fight against ransomware, she said.
She also announced the Joint Cyber Defense Collaborative (JCDC), which was celebrated on screen with an AC/DC style logo and some dancing on the part of the director. "I wanted to call it the Advanced Cyber Defense Collaborative, but the lawyers wouldn't let me," she quipped.

According to Easterly, the JCDC will gather public and private sector security experts to share information, plan for worst case scenarios, and then carry out those plans when necessary. "You have to plan in peace time so you're ready in war time," she said.

Initial participants in the JCDC will include AT&T, AWS, CrowdStrike, FireEye, Google, Lumen, Microsoft, Palo Alto Networks, and Verizon

Easterly also outlined how CISA is working to bring more workers into cybersecurity, and made a pitch for employment at CISA. She called on attendees to help educate the general public on important security issues. "If we can collaborate together we can raise that cyber security baseline," she said.

Despite its position in the security industry, Black Hat doesn't usually host high-profile government speakers. The most notable exception was General Keith Alexander, then NSA chief, who appeared in 2013 in the wake of the Snowden leaks, who got a pretty chilly reception (and reportedly risked being egged).

But Easterly's statements come at a time of increasing government visibility in the world of cybersecurity. Earlier this year, Anne Neuberger, the Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology on the NSC, addressed the RSA Conference on the impact of post-release patching on national security.

# 45. Algorithm Speeds Monte Carlo Predictions on Quantum Computers

by Kimberley Mok
https://thenewstack.io/algorithm-speeds-monte-carlo-predictions-on-quantum-computers/

In a world where the uncertain specter of climate change and a global pandemic dominate the headlines, being able to accurately predict potential outcomes can help us better determine which is the best path forward in any given scenario. While the practice of forecasting has been around since ancient times, it’s only in the last several decades that computers have made their mark in the field by propelling data-driven methods of predictive analytics.

One of the most well-known class of computational algorithms for tackling such predictions are Monte Carlo methods, which are used to model the probability of different outcomes when random variables play a role. But running these models can be computationally intensive, and present a challenge to the computational limits to today's binary-based "classical" computers. Thus, the next logical step is a transition to using more powerful quantum computers in order to more quickly and accurately model the full spectrum of complexity inherent in today's most pressing problems.

## Quantum Speed-Up

In a recent breakthrough that will give the nascent quantum computing industry a boost, UK-based startup Cambridge Quantum Computing has developed a new algorithm that demonstrates a considerable speed-up in how these predictions can be performed, which was detailed in a recent pre-print paper.

"Monte Carlo methods are extremely widespread in science and business — basically, any time some reasoned decision must be made in the face of uncertainty, the chances are that a Monte Carlo method is being deployed," explained Dr. Steven Herbert, a senior research scientist at CQC. "This includes applications ranging from weather forecasting, to designing particle-physics experiments in the Large-Hadron Collider, to deciding who to award the victory to in a curtailed sporting event (for example, using the Duckworth-Lewis Method in cricket) — and indeed the pricing of sports betting markets."

In particular, Herbert's work focused on a technique known as Monte Carlo integration, which is used by banks, asset managers, hedge funds, and financial planners to do things like option pricing and risk analysis.

"'Monte Carlo integration' is really just a grandiose name for sampling from some probability distribution (for example, when we roll a dice we uniformly 'sample' a number between one and six) and then averaging the samples to approximate the mean," said Herbert. "However, this simple process is remarkably computationally intensive, and so the fact that there is quadratic quantum speed-up available (quadratic means the quantum algorithm will complete in about square-root of the time it would have taken classically) makes it an extremely attractive prospect to become one of the first applications to see a real useful quantum advantage."

Typically, Monte Carlo simulations run on "classical" computer systems can take hours — sometimes even overnight — to complete. By that time, the results of the simulation may already be obsolete. While basing important decisions on outdated results may not have a huge impact on things like optimizing delivery times in supply chains, it can sometimes mean the difference between life or death when strategizing during critical events like a pandemic.

In contrast, CQC's new algorithm leverages the ability of quantum computing to model an increased number of random values in a simulation, thus augmenting the scale and accuracy of predictions. It does this by using a hybrid approach, where a portion of the simulation is run on conventional computing systems, and another portion performed using quantum computers, thus striking a balance between the operational cost-efficiency of classical systems, and the increased accuracy and considerable computational power of quantum systems.

"Every method of quantum Monte Carlo integration has a theoretical 'quadratic' quantum advantage over classical Monte Carlo," said Herbert. "However, before this breakthrough, in order to do quantum Monte Carlo integration you also had to perform 'arithmetic' operations like inverse-sine and square-root on the quantum computer. Doing so offers no intrinsic quantum advantage, however, and nobody had figured out how to offload these operations to a classical computer. That's what I did, and if we are to see useful quantum advantage in the 'NISQ era' (that is, while quantum computers are still 'noisy' and resource-constrained), then it is absolutely crucial to use the quantum computer only for the precise operations where it gives a computational advantage. Otherwise, the quantum state will decohere before the computation is complete, rendering the results unreliable."

Broadly speaking, this hybrid approach of combining both classical and quantum systems isn't new within the industry, with companies like Microsoft and IBM offering their own composite platforms. While quantum computing can offer a remarkable boost over classical computers in solving most complex computations, there are still situations where classical computers can still edge out an advantage over their more error-prone quantum counterparts. In this sense, CQC's hybrid technique offers a win-win solution to a difficult problem, which had not been available before.

"This proposed algorithm is the state-of-the-art in quantum Monte Carlo integration," said Herbert. "It can solve any Monte Carlo integral with the full quadratic quantum advantage while using the quantum computer only for those operations where there is quantum advantage. None of the other approaches achieve all of these."

Herbert added that the recently announced partnership between CQC and Honeywell Quantum Solutions (HQS) will mean more closely coordinated improvements in the development of quantum hardware and software in the future, particularly when it comes to enhancing the implementation of quantum Monte Carlo integration.

"I look forward to working together with the experimentalists and hardware engineers to pinpoint and remedy the precise ways in which algorithms are 'resource constrained' when executed on actual quantum hardware, and hence, remove obstacles in the path to quantum advantage. In principle, this approach really is the 'best of all worlds', however, in practice there are still application-specific refinements that can be made. That's our next job: to find partners who are keen to explore the transformative effects that quantum Monte Carlo integration will have on problems relevant to their business, and to engineer tailored solutions."

# 46.51 CTOs Transforming The World of Quantum Tech

by James Dargan
https://thequantumdaily.com/2021/08/05/11956/

A chief technology officer (CTO) is one of the most important roles in any tech company. Sometimes the head of engineering, at other times not, the CTO has to be an excellent engineer while also possessing the required skills to communicate complicated technical issues to people from non-technical backgrounds, C-suite executives, for instance.

They must be experts in company policy and procedures and have enough intuition to know which direction the company needs to head.

For a quantum technology company—one of the hardest of deep tech niches—this is more important than ever. Skills in communication, leadership, finance and business development must meld with the technical side of things to create the required dynamism necessary for a successful company.

Realizing it's usually the CEOs and presidents who get to bask in all the limelight, *TQD* thought it time to mention those CTOs in the deep and dirty trenches, the people who—in essence—make the startups and companies tick on a day to day basis.

One thing to note, however, is that as usual, this list is non-exhaustive. I have only mentioned those enterprises that actually have the title of CTO as a position in their corporate structure.

## Semantics & Diversity Issues

Companies like Google, IBM and other big players, as well as dozens and dozens of QC startups, do—for whatever reason—use different titles such as chief scientific officer (CSO) or chief innovation officer (CIO) etc when applied to positions when the role is similar to that of a CTO in their respective organizations, but semantics aside, the list has been collated to highlight those important people in their CTO roles rather than to cause injury to those not included.

One major disappointment in compiling this list has been the lack of diversity—as expected, white men abound. Women, well, that's an embarrassing shame, with Elena Blokhina and Prineha Narang being the only representatives on the list. The list is given below:

**Arman Zaribafiyan:** CTO at 1QBit, **Scott Dufferwiel:** CTO at AEGIQ, **Matteo Rossi:** CTO at Algorithmiq, **Prineha Narang:** CTO at Aliro, **David Bestwick:** CTO at Arqit, **Christian Nietner:** CTO at Avanetix, **Rut Lineswala:** CTO at BosonQ Psi, **Yehuda Naveh:** CTO at Classiq, **Dana Anderson:** CTO at ColdQuanta, **Oliver Maynard:** CTO at Crypta Labs, **Jean-Charles Faugère:** CTO at CryptoNext Security, **Stephen Lyon:** CTO at Ee-roQ, **Ewan Munro:** CTO at Entropica Labs, **Elena Blokhina:** CTO at Equal1.labs, **Norbert Lütkenhaus:** CTO at EvolutionQ, **Jungsang Kim:** CTO at IonQ, **Kuan Yen Tan:** CTO at IQM Finland, **Mike Brown:** CTO at ISARA Corporation, **Thomas Decker:** CTO at JoS Quantum, **Philip Sibson:** CTO at KETS Quantum Security, **Jan Spallek:** CTO at Kiutra, **Samuel Mugel:** CTO at Multiverse Computing, **Bill Shipman:** CTO at POLARISqb, **Tomas Babej:** CTO at ProteinQure, **Robert Love:** CTO at Q-CTRL, **Svetoslav Sotirov:** CTO at Qaisec, **Jules van Oven:** CTO at QBLOX, **Jean-Philippe Bourgoin:** CTO at QEYnet, **Felipe Favaro de Oliveira:** CTO at Qnami, **Robert Stockill:** CTO at Qphox, **Denis Mandich:** CTO at Qrypt, **Vincent Elfving:** CTO at Qu & Co, **Niccolo Somaschi:** CTO at Quandela, **Nitzan Livneh:** CTO at Quant LR, **Michael Redding:** CTO at Quantropi, **Yonatan Cohen:** CTO at Quantum Machines, **Jon Ander Oribe Sánchez:** CTO at Quantum Mads, **John Morton:** CTO at Quantum Motion, **Douglas Birch:** CTO at Quantum Trilogy, **Shahryar Shaghaghi:** CTO at Quantum Xchange, **Duncan Earl:** CTO at Qubitekk, **George Siopsis:** CTO at Qubit Engineering, **John Leiseboer:** CTO at QuintessenceLabs, **Jelmer Renema:** CTO at QuiX, **Mael Flament:** CTO at Qunnect, **Vivek Shenoy:** CTO at QNu Labs, **Kostantin Vilk:** CTO at QuSecure, **Oleg Mukhanov:** CTO at SeeQC, **Robert Bedington:** CTO at SpeQtral, **Valerii Vinokur:** CTO at Terra Quantum, **Yudong Cao:** CTO at Zapata Computing

# 47. QUANTUM COMPUTING: CHALLENGES AND OPPORTUNITIES AHEAD

by Madhurjya Chowdhury
https://www.analyticsinsight.net/quantum-computing-challenges-and-opportunities-ahead/

Google stated in 2019 that it has achieved quantum supremacy, a milestone in which quantum machines solve problems that conventional computers cannot solve in an acceptable period of time. Companies such as Amazon Web Services (AWS), Microsoft, and IBM have also created quantum computing cloud platforms, which offer the potential of quantum computing to consumers who may utilize the services without owning the physical hardware.

Nevertheless, while perfectly functioning quantum computers appear to be just around the edge and will be easy to access to the organization, there are still a number of quantum computing challenges to overcome, including accuracy and fault tolerance, which might take at least four to five years to ensure its credibility.

Nonetheless, quantum computing is having a big influence on the workplace and IT executives must remain on top of the developments.

Let's take a look at the challenges and opportunities of Quantum Computing in the coming years.

## What is Quantum Computing?

Quantum computers are data storage and processing devices that make use of quantum mechanics. This may be highly beneficial for some jobs, where they can substantially outperform even our most powerful supercomputers.

Data is stored in binary "bits," which can be either 0s or 1s, in traditional computers like laptops and smartphones. A quantum bit, or qubit, is the fundamental memory block of a quantum computer.

## Influence of Quantum Technology on Security

Quantum computing poses a challenge to conventional encryption methods, which are incapable of dealing with quantum superpowers. And that's why the shift to quantum-safe algorithms must occur immediately.

"Quantum will alter the architecture of computer security, rendering many existing methods used for encryption and digital signatures practically worthless," Chris Hickman, chief security manager of digital identity security firm Key Factor, stated. "IT leaders must devise a strategy to protect their businesses as well as a practical plan to mitigate the inescapable arrival of quantum computing."

Hickman feels that the present encrypted assets must be re-evaluated and protected in a quantum-resistant manner. If it is not accomplished now, a lot of opportunities will be lost, and it will be too late or too expensive to safeguard them in the future.

## What is the Monetary Value?

Quantum computing is still in its development, with many unresolved difficulties, but it is an area that will transform sectors such as banking, medicine, automobiles, and artificial intelligence in the next few years. Organizations must stay up in order to maintain a competitive advantage.

"IT executives should focus on quantum computing right now," said Nir Minerbi, CEO of Classiq, the first Israeli firm in the sector of quantum computing software. "Rivals have already arrived, collecting quantum algorithms and proprietary information that will provide them a major competitive advantage in the years ahead."

As per Christopher Savoie, president and Chairman of Zapata Computing, which develops quantum computing software, it will be difficult for businesses that are not quantum-ready to keep up.

He believes that advances in quantum computing will have a disruptive influence on every major sector.

Financial services firms and other industries that rely significantly on statistical modeling of future events, for example, will profit from quantum's capacity to do computations in ways that go beyond conventional capabilities.

Companies in the pharmacological and information sciences will accelerate the discovery of new organic compounds and molecules by being able to simulate quantum encounters that are difficult to simulate precisely on classical computers or to execute quantum-enhanced artificial intelligence to extract correlations in information.

"If quantum computing is going to impact your sector, the rate of acceleration implies IT executives need to start thinking about quantum investments now," Savoie added.

Minerbi remarked that, aside from the rate of acceleration, quantum algorithms are beneficial for another reason: "Fault-tolerant quantum computers are certainly 10 years away, but good quantum algorithms that might be performed on noisy quantum computers are present, and now is the ideal moment to create them."

## Quantum Computing as it is Now

In its current condition, quantum technology is being used in several projects. In 2020, IBM and Daimler utilized a quantum computer to simulate the dipole moment of 3 lithium-containing molecules, putting us one inch ahead of next-generation lithium-sulphur batteries that are more powerful, last longer, and are less expensive than today's commonly used lithium batteries. IBM has collaborated with JPMorgan on quantum use factors in finance, such as research into the use of quantum computing to valuation models. However, quantum technology isn't just for computers.

"It's essential to remember that many devices on the market today, including mobile phones, involve quantum phenomena," said Deborah Golden, Deloitte's U.S. cyber and strategy risk head. "While current quantum use cases are restricted," she added, "They are increasing." Quantum communications, for example, provide substantial security against eavesdropping.

## Getting ready for Quantum Future

Understanding the problems of quantum computing is only one-half of the equation, as quantum is a world apart from what businesses are used to.

"Unlike conventional computers, quantum computers only offer a likely response," said Vaclav Vincalek, an entrepreneur who assists businesses in implementing cutting-edge technology.

They aren't designed to deliver definite results; instead, the response they present is the most likely, which may require verification by a traditional computer. For instance, a quantum computer may calculate the most likely solution for cracking an encryption scheme, but it will require a classical computer to test the solution to see whether it starts breaking.

As a result, coding for quantum technology is a novel problem. There was no straightforward method to move or reuse code between systems before there existed a real quantum operating system.

## Conclusion

While quantum computing has the enormous potential to revolutionize how real-world issues are tackled, there are still numerous difficult engineering challenges to overcome first, leaving companies without a timeframe for when it will be used in the workplace.

# 48. AWS taps up Singapore scientists to overcome hurdles facing quantum computing

by Laura Dobberstein
https://www.theregister.com/2021/08/05/aws_quantum_singapore/

Amazon Web Services has partnered with the National University of Singapore (NUS) in hope of improving quantum technologies and their applications. The duo announced they had signed a Memorandum of Understanding this week.

The collaboration will be led by the NUS-hosted Quantum Engineering Program (QEP), a five-year SG$25m ($18.5m, £13.3m, €15.6m) initiative launched in 2018 by Singapore's National Research Foundation that focuses on translating the often abstract science of quantum physics into tech that can be commercialized.

So far, the QEP has supported eight major research projects – such as hardware and software that may be able to eventually outperform today's supercomputers and simulate chemicals to help design drugs – though these solutions remain unfinished, waiting until future-gen quantum computers can make them a reality.

"The QEP is currently working with companies to identify problems they face that quantum technologies may already or may soon be able to tackle," QEP director Alexander Ling told *The Register*.

"For example," said Ling, "it will support quantum computing software researchers to investigate algorithms and simulation techniques that could be applied to real data. Proposals aimed at tackling challenges in supply chain management, finance, trading, chemistry and materials are currently under review for funding."

Quantum computing may one day be able to provide powerful computational tools beyond the reach of traditional computers, though producing a practical system will likely require leaps in science and engineering. And if quantum computers do take off – they're still in the science experiment stage – you'll want your communications to be quantum-secured: these computers may be able to computationally crack non-quantum-secured data.

"Some forms of encryption used today can be broken by future large-scale quantum computers, which also drives a search for alternatives," Ling said.

In a canned statement, the NUS said AWS will gain access to the university's National Quantum-Safe Network, a vendor-neutral platform for developing technology and integrating some of it into local fiber networks.

"The understanding that we are using quantum communications technology to support experiments using existing fiber is correct," AWS ASEAN managing director Tan Lee Chew told *The Register*.

Tan said AWS sees opportunities in supporting Singapore's Smart Nation initiatives, such as traffic optimization, financial planning, shipping and port operations, and materials design applications within commercial organizations.

“Quantum technologies have the potential to help Singapore accelerate its Smart Nation agenda,” said Tan, adding: “The goal is to train academics, students, and commercial organizations in Singapore to be skilled in quantum computing, including he ability to then develop their own products.”

Inevitably, there will also be some joint public-relations activities.

Last August, AWS debuted a cloud-based quantum-computing-ish service the tech giant called “accessible, affordable and easy to use” named Braket. The pay-only-for-what-you-need product provides access to quantum annealers; gate-based systems built on superconducting qubits and on trapped ions; and hybrid quantum and classical algorithms tools. Users work in the Jupyter notebook environment.

Quantum cloud endeavors are not new: IBM and Microsoft are already doing it. In fact, IBM is already in the middle of a three-year collab with QEP in which Big Blue provides NUS researchers cloud access to 15 of IBM's current-gen quantum-computing systems.

As for the massive machine that is AWS, Ling said there was already an existing relationship: "Researchers in Singapore already had some links to the companies working with AWS to offer cloud access to quantum hardware.”

# 49. Hackers target Kubernetes to steal data and processing power. Now the NSA has tips to protect yourself

by Liam Tung
https://www.zdnet.com/article/hacker-target-kubernetes-to-steal-data-and-processing-power-now-the-nsa-has-tips-to-protect-yourself/

The National Security Agency (NSA) has released its first Kubernetes hardening guidance to help organizations deploy the open-source platform for managing containerized applications.

The guidance was also authored by the DHS's Cybersecurity and Infrastructure Security Agency (CISA) to make users aware of key threats and configurations to minimize risk.

"Kubernetes is commonly targeted for three reasons: data theft, computational power theft, or denial of service," the agencies note in a joint announcement.

"Data theft is traditionally the primary motivation; however, cyber actors may attempt to use Kubernetes to harness a network's underlying infrastructure for computational power for purposes such as cryptocurrency mining.”

Researchers recently warned that attackers were using misconfigured Kubernetes deployments to drop crypto-miners on enterprise hardware.

The key hardening guidance isn't unusual, but the report also offers an in-depth look at applying standard security mitigations in the context of complex environments that are often deployed in the cloud. At a high-level the guidance

includes: scanning containers and pods for vulnerabilities or misconfigurations, running containers and pods with the least privileges possible, and using network separation, firewalls, strong authentication, and log auditing.

Of course, standard cyber hygiene is key too, including applying patches, updates, and upgrades to minimize risk. They also recommend vulnerability scans to check patches are applied.

The advice covers Kubernetes clusters, the control plane, worker nodes (for running containerized apps for the cluster), and pods for containers that are hosted upon these nodes.

The NSA and CISA make a special point about supply chain risks, including software and hardware dependencies that could be compromised at any point in the supply chain before deployment.

"The security of applications running in Kubernetes and their third-party dependencies relies on the trustworthiness of the developers and the defense of the development infrastructure. A malicious container or application from a third party could provide cyber actors with a foothold in the cluster," the agencies note.

The report also warns that remote attackers do target control plane components lacking appropriate access controls, as well as worker nodes that live outside of the locked down control plane.

Insider threats include admins with high privileges and physical access to systems or hypervisors.

Pods in particular need to be hardened against exploitation because they're often an attacker's initial execution environment after exploiting a container.

It also recommends running non-root containers and rootless container engines to prevent root execution as many container services, by default, run as the privileged root user.

# 50. Post-quantum chip has built-in hardware Trojan

by Christoph Hammerschmidt
https://www.eenewseurope.com/news/post-quantum-chip-has-built-hardware-trojan

Hacker attacks on industrial plants are no longer fiction. Attackers can steal information about production processes or paralyse entire factories. To prevent this, chips in the individual components of the plants already communicate with each other in encrypted form. However, many encryption algorithms will soon no longer offer protection: While today's computers cannot crack established procedures, quantum computers would certainly be able to do so. This is especially critical for durable devices such as industrial plants.

For this reason, security experts worldwide are working feverishly to develop technical standards for post-quantum cryptography. One of the challenges here is the high computational demands of these encryption methods. A team led by Georg Sigl, Professor for Security in Information Technology at TUM, has now designed and had manufactured a chip that implements post-quantum cryptography particularly effectively.

Sigl and his team rely on a hardware-software co-design. In this process, specialised components and control software complement each other. "Our chip is the first to consistently rely on a hardware-software co-design for post-quantum cryptography," says Prof. Sigl. "As a result, it can implement encryption with `**Kyber**' — one of the most promising candidates for post-quantum cryptography — about ten times as fast as chips that rely on pure software solutions, consumes about eight times less energy and is almost as flexible as them".

The chip is an application-specific integrated circuit (ASIC). Such specialised microcontrollers are often manufactured in large numbers according to the specifications of companies. The TUM team modified an open-source chip design based on the open-source RISC-V standard. This de facto standard is becoming more widespread and could replace proprietary approaches by large companies in many areas. The chip becomes post-quantum cryptography-capable on the one hand through a modification of the computing core and specific additional instructions with which necessary computing operations are accelerated.

In addition, the design was expanded to include a specially developed hardware accelerator.

This not only enables the processor to use so-called lattice-based post-quantum cryptography algorithms such as Kyber, but could also work with the SIKE algorithm. This is associated with significantly more computing effort. According to the team, the chip developed at TUM can implement this algorithm around 21 times faster than chips that rely on software for encryption. Among experts, SIKE is seen as a promising alternative should grid-based approaches prove to be no longer secure at some point. Such safeguards make sense wherever chips are used over a long period of time.

In addition to the number of conventional hacker attacks, the threat from hardware Trojans is also increasing: computer chips are usually manufactured according to the specifications of companies in specialised factories. If attackers manage to smuggle Trojan circuits into the chip design before or during production, this could have serious repercussions. Just as with a hacker attack from outside, factories could be paralysed or production secrets stolen. What's more, if the Trojan is already built into the hardware, it could also be used to subvert post-quantum cryptography.

"So far, we know very little about how hardware Trojans are used by real attackers," explains Georg Sigl. "To develop protective measures, we have to put ourselves in the shoes of attackers, so to speak, and develop and hide Trojans ourselves. That's why we have built four Trojans into our post-quantum chip that we developed and that work quite differently".

In the coming months, Sigl and his team will intensively test the cryptographic capabilities of the chip and the function and detectability of the hardware Trojans. Afterwards, the chip will be dismantled - for research purposes. In an elaborate process, the conductor paths are ground down layer by layer, each individual layer is photographed. The goal is to test new AI methods that can be used to reconstruct the exact functioning of chips, even if no documentation is available. "Such reconstructions can help identify components of a chip whose function has nothing to do with its actual tasks and which may have been smuggled in," says Sigl. "Such methods could one day become standard for spot checks in large chip orders. Together with effective post-quantum cryptography, we can thus make hardware in industrial plants, but also in vehicles, more secure".

# 51. Quantum Randomness Now Boosts Everyday Security

by EDD GENT

https://spectrum.ieee.org/quantum-randomness-boosts-everyday-security

Randomness is typically seen as a problem, interfering with our ability to make sense of the world and complicating our attempts to predict the future. But that very unpredictability also makes it a crucial ingredient in the encryption that protects billions of dollars worth of private data. Random numbers are used to make cryptographic keys, and any latent pattern in the key can be used to crack encryption. True randomness is harder to come by than you might think though, which is why people are increasingly turning to the strange world of quantum mechanics to find it.

Chinese tech giant Alibaba recently published research on a quantum random number generator (QRNG) platform that it has been using to enhance the security of its cloud as well as financial services like Alipay and Ant Financial. And in April, Samsung released the Galaxy Quantum 2 — the second generation of its new line of smartphones secured using a specialized QRNG chip.

Others may soon follow in their footsteps, says Axel Foery, an executive at Swiss company ID Quantique, which supplies QRNG chips used by both Alibaba and Samsung. He says they are in discussions with a number of major cloud-providers and leading smartphone makers and he thinks the use of quantum randomness could soon be standard practice. That's because ever more powerful computers and new techniques like machine learning and quantum computing are making traditional sources of randomness increasingly easy to hack, he says.

"It's still some effort, but it's less effort than it was in the past," he adds. "And if you understand the randomness and you can predict it then you have no randomness. And then you can manipulate all the functions that rely on this randomness."

It's possible for computer to generate random numbers by harnessing environmental processes such as thermal noise in a computer chip or a user's mouse movements. But this can be too slow for many applications, and there are typically biases in the way these phenomena are measured that reduce their randomness.

As a result, most encryption today relies on pseudo-random number generators, which use algorithms to produce numbers with statistical properties close to random. But any "random" number generated by a mathematical process is inherently deterministic, says Foery, and if you can crack how it works you can predict any security key it produces.

Quantum processes on the other hand are inherently probabilistic. Even with perfect information its impossible to predict their outcome exactly. One of the most popular way of harnessing this quantum randomness is to fire light at a beam splitter. The chances of an individual photon going one way or the other are 50-50, so by counting the number of photons that land either side you can generate a string of random binary bits.

This approach has the benefit of being able to generate random numbers much faster than alternatives, says Foery and is the technique used by ID Quantique. And while such devices used to be bulky and expensive, rapid improvements in the ability to integrate optical components with silicon means their latest chips are just 2.5 millimeters across. Prices have also dropped significantly and Foery estimates their chip only represents a few percent of the overall production cost of the Galaxy Quantum 2.

Whether your average smartphone user needs the extra security provided by a QRNG is debatable. But Juan Carlos García Escartín, an associate professor at the Universidad de Valladolid in Spain who studies quantum information, says the fact they are now making it into consumer products is a promising sign the technology is breaking out of niche applications. "I wouldn't have expected a few years ago that something you can buy in a store will have a QRNG inside," he said.

The platform outlined by Alibaba in their recent Nature paper is even more intriguing though, he says. The system combines three commercial QRNGs, including one from ID Quantique, with a QRNG made by the company's own researchers. The system has been used to deliver random numbers to a variety of applications running on the company's cloud for more than a year. Alibaba declined an interview request.

The paper's authors describe how combining output from the QRNGs in different ways lets them tune the level of security provided and the speed with which numbers can be generated, which is important for a cloud server that has to generate large numbers of security keys."Their servers will be connecting to millions of users," says García Escartín. "These quantum devices can be very fast and that's something that, if you are on a daily basis working with huge amounts of randomness, would be very interesting." However, sending random numbers from a central server to other applications running on the cloud is potentially risky, he says, because an attacker could potentially intercept them.

Generally you want to generate your random numbers at the same location that you generate your security keys to avoid this risk, says Roger Colbeck, a professor at the University of York in the UK who studies quantum information. "If they're using some method to get them from their server to the user that could be hacked then they're kind of compromising the 'quantumness' of their random numbers," he says.

In that respect, integrating QRNGs into users individual devices may be a more secure approach. But given the still considerable cost, how many manufacturers are ready to do away with conventional random number generators remains to be seen.

"Whether they're quantum or not is really a question of a money and security trade-off," he says. "But if manufacturers really get into competition, there's a real drive towards miniaturization and costs get reduced I don't see why in 10 years time every computer you buy couldn't have a little QRNG inside."

# 52. HQS Quantum Simulations releases backend extending its library to support AQT's trapped-ion quantum computers

by Thomas Monz
https://quantumsimulations.de/news/hqs-quantum-simulations-releases-backend-aqt

The steady development of quantum technologies is bringing their promise closer and closer to the market, as companies around the world aim to deliver their quantum enhanced solutions to the general public. In a bid to allow developers everywhere to participate and use quantum computers, HQS Quantum Simulations has announced the release

of a library connecting its open source quantum computing library, qoqo, to AQT's quantum simulators, with an intended complete support of their trapped-ion quantum computers in the future.

As the physical limits of conventional computing are starting to appear in many R&D labs around the world, quantum computing is considered to be the natural way forward for resource-intensive tasks that are currently pursued using high performance computing (HPC) clusters: physical, chemical, and manufacturing simulations are all expected to move on to quantum computing in the coming decades.

Yet, the path ahead is rife with obstacles, as experimental realizations of quantum bits, or qubits, the fundamental components of quantum computers, are notoriously difficult to achieve. The useful quantum properties of qubits are fragile and very easily lost when they are exposed even to the tiniest disturbances in their surroundings, leading to the phenomenon known by physicists as decoherence. Currently, various hardware approaches are pursued to realize inherently resilient qubits. Quantum computers based on trapped ion technology are promising in various respects: compared with other architectures, trapped ion quantum computers have a strong advantage when it comes to qubit connectivity, and gate fidelity. Ion traps have been central in the pioneering of several milestones in quantum information processing and they have become the platform on which the most complex quantum algorithms have been performed; the team at AQT has made several contributions to these outstanding achievements.

HQS Quantum Simulations has been developing qoqo, a quantum circuit representation library which empowers developers to build quantum circuits and run them on different backends. The latest addition comes with the connection of AQT's technology to qoqo. Users are now able, without any modification to their existing circuits, to run them on AQT's quantum simulators, both with and without noise. This marks a helpful technical accomplishment as a sound stepping stone for future implementation of AQT's quantum hardware as a qoqo backend.

"Our partnership with AQT is valuable to us," said HQS CEO Michael Marthaler. "Connecting qoqo to their hardware stack was always in our sights. Ion traps open huge opportunities when it comes to realizing practical quantum computing."

# 53. How post-quantum cryptography will save us in the age of quantum computing

by Robert Scammell
https://www.verdict.co.uk/post-quantum-cryptography-safety/

In research labs around the world, a race is playing out between engineers building a completely new kind of computer and the cryptographers creating encryption tools to protect us from the superior computing power. Here's why businesses should start thinking about post-quantum cryptography now, and the steps they can take to keep safe.

Fully scaled quantum computers, which will rip up the computing rulebook, are still some way off: some experts say it will be another 10 years before we see at-scale, error-free quantum computers, while more conservative estimates put this figure closer to 30.

But recent advances, such as Google's claim to quantum supremacy – when a quantum computer solves a problem that a classical computer is unable to – have underscored how their radically different approach can upend computing.

Quantum computing (QC) is usually explained by saying that where a normal computer operates using bits of information, a quantum computer uses quantum bits or "qubits". A normal bit is 1 or 0, on or off: a qubit is much more complicated. When it is measured it will be either 1 or 0; before that, it exists in a quantum superposition of those two states. The quantum superposition is usually described using "complex numbers", mathematics based on the so-called "imaginary unit", the square root of minus one.

Another way of visualising this is that normal bits are like coins lying on a table. They are either heads or tails up: they can be flipped over. A qubit, however, is like a coin spinning in the air. It can interact with other spinning coins, affecting how they spin, but none of them are heads or tails up until the quantum operations are complete.

Theoreticians can describe what qubits will do in a network of quantum logic gates, even if they don't have any actual machinery capable of carrying out the process. As a result, algorithms can be, and have been, developed for QC machinery even before there was any – rather in the way that Ada Lovelace famously wrote some of the first conventional computer programs for Charles Babbage's proposed 19th-century mechanical computer, the Analytical Engine, even though it was never actually built.

Thus we know many of the things that QC could achieve. Its effects, when it becomes available at appropriate scale, will be enormous. Quantum computers will find a use anywhere there is a large and complicated problem to be solved. That could be anything from predicting the financial markets, to improving weather forecasts, to cracking encryption systems.

The turbo-charged computing power of quantum computers is expected to make mincemeat of many of our current encryption tools, which we depend on every day to keep our messages private and know that the machines we communicate with are legitimate.

To understand how quantum computers will be able to crack today's encryption, it's worth considering how cryptography works today.

There are two commonly used types of cryptography: symmetric and asymmetric. It is asymmetric cryptography that is at risk from quantum computers. Its algorithms consist of two mathematically linked keys – a private and a public key. The public key encrypts, while the private key is known only by the party decrypting the information.

Asymmetric cryptography is the most used in day-to-day communication, with many types of encryption falling under this umbrella. Perhaps the most widely used is RSA, which is used to secure web browsers, chat applications, VPNs and more. These algorithms are based on a complex maths problem known as prime factorisation. The longer the key – the more bits – the harder it is to replicate the maths and so break the encryption.

Current computers do not have the computing power to break the RSA algorithm. But we know that it will be possible with quantum computers thanks to Shor's algorithm, devised by Peter Shor in 1994.

And by factoring these numbers on a quantum computer, an attacker will be able to reverse engineer, or factor, the private key.

"It's not breaking the encryption. It is breaking the keys," says Kevin Bocek, vice president of security strategy & threat intelligence at Venafi, a cybersecurity firm protecting machine identities.

## Post-quantum cryptography: It's not all about the qubits

The rough estimate is that two qubits per bit of the key are needed to break the encryption. So for RSA 2048, a quantum computer would need 4,096 qubits. But it's not quite that simple, says IBM cryptographer Vadim Lyubashevsky, who has been working on the post-quantum cryptography problem since 2002.

"Just measuring qubits is somewhat deceptive," he says. That's because these estimates refer to a logical qubit that is free from the errors that today's fledgling quantum computers are very much prone to.

He continues: "Unfortunately when you're building a quantum computer, things are very unstable. So in order to create one of these logical qubits, we may need, say, 1,000 actual physical qubits."

IBM's most powerful quantum computer currently boasts 65 qubits, while Google's has 72. All of these are far from the perfect, error-free logical qubit.

But computer scientists are working to improve these numbers. And when a fully functioning quantum computer with lots of qubits arrives on the scene, the security implications could be severe. A quantum computer could easily imitate the identity of another machine by replicating digital certificates such as SSL/TLS, which are used to tell us a computer is genuine.

"The risk is of a quantum computer being able to recreate these identities, these keys, essentially, out of thin air," says Bocek. "And one machine now could look like another machine, one machine could break our privacy. So now we could have a whole bunch of masquerading, marauding machines and so our private communications, whether we're a business or us personally – becomes known to everybody."

We've already seen the dangers of expired digital certificates. In 2017, hackers managed to steal 145 million customer records from Equifax undetected in part because of an expired digital certificate.

But in a post-quantum world, it won't be your average cybercriminal carrying out quantum attacks.

Despite the potentially serious implications of this looming threat, quantum computers will only be available to a small number of people. That's because they are incredibly difficult to build, requiring very specific parts, and will need to be kept in controlled lab environments. And they'll be expensive.

This means that they will remain firmly under the control of nation states, a small handful of large commercial entities and academic organisations.

Or, as Bocek puts it: "Terrorists can't conjure up a quantum computer with pieces ordered on eBay".

While they will likely remain firmly in the hands of powerful nation states, there is no guarantee that they won't ever be used as part of a cyber-arsenal to further strategic goals.

"So whether that is eavesdropping, spying on a certain set of adversaries, or whether a nation state wanted to convey this as a weapon to destroy or create havoc in commerce – that's the way that these will be used," says Bocek.

"Another type of attack may be to create havoc and uncertainty. A nation state might look to create distrust maybe in the banking or financial systems as retribution. And so, be able to masquerade or change certain trades or banking operations."

In extreme cases, they could hypothetically be used to disrupt banking operations an trigger a recession, adds Bocek.

Professor Michele Mosca, co-founder and deputy director of the Institute for Quantum Computing at the University of Waterloo, says that if adequate defences aren't developed in time, then "critical IT infrastructures will fail with no quick fix. Unlike today's hacks, where we detect and remediate as quickly as we can, in this scenario the new tools needed to remediate haven't yet been developed".

And if they are developed but not robustly deployed in time in the real-world, "migration will be managed as a crisis," says Mosca.

"This will be disruptive, expensive and worst of all lead to very bad designs and implementations. Bad designs and implementations can be hacked without a quantum computer."

## Defending against quantum attacks

In 2017, Mosca estimated that there's a one in six chance of quantum computers being able to break RSA 2048 by 2027. So, what can be done to defend against quantum attacks?

Some algorithms cannot be cracked by Shor's algorithm, such as SHA-256, which is used in hashing for securely storing passwords, or AES, which is used to encrypt files and hard disks.

But these cannot be used for machine identities or to encrypt web communications. Instead, we will require new encryption tools that are based on different mathematical principles to defend against a quantum attack.

These will be bigger and larger keys, ones that are immune to quantum attacks. So how close are we to having these quantum-safe algorithms?

"These fundamental low-level tools already exist," says Mosca. "But they aren't deployed widely in real-world systems."

Tech heavyweights such as Google, IBM and Microsoft are among the players developing these. Other companies, such as Thales, have announced plans to develop quantum-safe algorithms.

As GlobalData thematic analysts note in a quantum computing report: "Most observers believe that in the time it will take to develop a quantum computer sufficiently powerful to run Shor's algorithm at a scale advanced enough to threaten encryption, the cybersecurity industry will develop quantum-resistant encryption."

Lyubashevsky says that post-quantum cryptography is already here and we can be "reasonably certain of their security". At IBM he helped develop three sets of post-quantum cryptography algorithms: Crystals Dilithium, Crystals Kyber and Falcon.

"It's just a matter of being standardised," he says. "And they're already being used in some parts. Anyone can use them."

But Mosca says that while – by some interpretations – we have these algorithms today, they haven't been scrutinised enough yet.

"At the other end, one might argue we're at least a decade away from robust, widescale, standardised deployment of quantum-safe crypto in critical real-world systems," he says.

## Leading the quantum resistance

The beacon for all these efforts and the body deciding the next encryption standards is the National Institute of Standards and Technology (NIST). The US government organisation is running a 'competition' to determine a handful of quantum-safe algorithms that will become the new standards.

NIST is experienced in managing encryption standards, having created the standards for all the previous encryptions and replacing them when they are cracked, all by a deadline.

Despite learning from the previous changes, it's "not easy", says Dustin Moody, the mathematician overseeing NIST's post-quantum cryptography standards competition.

"It's very, very slow, and you never completely get rid of the older [cryptography standards]," he says of the process of introducing new standards, adding that this time around it's "going to be somewhat of a more painful transition".

However, Moody is confident that the standards will be in place before large scale quantum computers start to threaten cryptography.

In June 2020, NIST narrowed the pool of potential encryption tools that will hold up in a post-quantum world down to a handful of cryptographic algorithms, with IBM's post-quantum cryptography making the cut.

The finalists have been selected on two criteria: security and performance. The process essentially involves researchers trying to break the post-quantum algorithms and making corrections where necessary.

Given that quantum computers are still in the nascent stage, researchers estimate "as best they can" how many operations a quantum computer would need to do to break it, says Moody.

These algorithms will also need to be able to withstand current decryption techniques and need to work in big computers, smartphones and smaller, IoT devices.

"We want quantum-resistant algorithms that can perform this sort of lightweight cryptography," Moody said in a NIST blog post.

Moody says that the aim is to narrow the quantum-safe tools down to a small handful to avoid confusion. NIST is aiming to publish these finalised standards in 2022, alongside guidance that explains the pros and cons of each type of quantum-safe encryption.

Once the standards are out, it will be down to industry to adopt them, knowing that the standards have the backing of the US government.

"These fundamental tools, even if standardised, need to be deployed in real-world systems," says Mosca. "This is not easy either, but some companies are taking serious steps."

Google, for example, has tested some post-quantum cryptography in Chrome, while Amazon, Microsoft, IBM and Cisco are among others that have been exploring it.

But a lot more needs to be done, says Mosca, and there is "broader complacency when it comes to cyber risk" among organisations.

"There is still a long hard road ahead, so we cannot be complacent," he says, adding that researchers will need to continue studying what "novel quantum attacks" may be used to compromise the proposed quantum-safe alternatives.

## What can businesses do to prepare for post-quantum cryptography?

So what, should businesses be doing right now when it comes to post-quantum cryptography?

Moody says that one of the main things is to "be aware of the threat" and know that a transition is on the horizon.

"We recommend that they do a kind of a quantum risk analysis, where they look at the cryptography that they're using right now," he says. "See what's vulnerable and what isn't, what public-key cryptography they're using; what their vendors are using; what products they're buying."

Bocek agrees that organisations should be carrying out an audit of their current encryption keys, adding that automation is one way to swap out the keys at scale.

And businesses don't necessarily have to wait for the standards, says Lyubashevsky. For example, a bank wanting to ensure its one-to-one transaction with its customers are quantum-safe today, it could put one of the algorithms on its mainframe to protect itself.

That's exactly what IBM is doing now with some of its customers, carrying out assessments to see if it's the right time to start migrating.

"There are right ways and wrong ways to incorporate these algorithms," adds Lyubashevsky.

He says the wrong approach is to take the post-quantum cryptography and simply hard code it into a system and be done with it.

"The better way is to do it in a very agile, modular way; to say, look, here's the place where our algorithm will go, we kind of know approximately how big the keys will be, we know how big the communication is going to be. And so then if you start migrating towards that type of architecture, and that type of security, it should be very easy to take whatever algorithms NIST will give, which will be some very small variation of what already has been submitted."

All of these approaches lead to a position known as being 'quantum agile', where it's easy to swap out old crypto for new post-quantum crypto.

But while quantum-safe cryptography is essentially already here and standardisation isn't far off, it's not time for businesses to relax.

## Record now, break later

For some time now, security experts have been worried about a concept known as 'record now, break later'. This means that anything currently encrypted with public key cryptography could be copied down now, stored, and decrypted when quantum computers are powerful enough.

"We need to have these standards in place as soon as possible because somebody could simply take your data right now and copy it down," explains Moody. "And it's encrypted using current public key cryptography. And then if a quantum computer comes out in 10 years, they could go back and decrypt your data."

"This is definitely the major worry right now, that somebody is harvesting data," agrees Lyubashevsky.

Of course, there's plenty of data that will be useless in ten or 15 years' time, or of no real security value. A message containing the family secret recipe to the perfect quiche is unlikely to draw the attention of a nation state, but for high-value data – be it medical patents or sensitive government cables – the hypothetical risk is too great to ignore.

And products such as satellites and trains with lifetime cycles of ten to 30 years that cannot be easily replaced once deployed, should be considering quantum-safe encryption.

That's why some organisations are already looking to implement quantum-safe encryption on their most valuable data now.

Mosca says that quantum key distribution (QKD) is one way to future proof against future quantum attacks. QKD "provides key agreement through a non-confidential but authentic channel (including a quantum channel)," he says. "QKD cannot be mathematically cryptanalysed, so it's resilient to 'record now break later' attacks."

Although QKD is commercially available now, it cannot provide digital signatures like RSA, so it isn't a silver bullet.

Above all, the main things for businesses to do now is be aware of the threat on the horizon, carry out an audit of their public encryption keys, keep an eye on NIST's standards, and aim to become quantum agile.

What happens when the next cryptography standards are here? Will they be the last upgrade, or will another algorithm or technology come along and break these post-quantum algorithms?

Lyubashevsky says breaking post-quantum algorithms is unlikely. Instead, it'll be that a faster, more efficient algorithm will come along and supersede the incoming generation of cryptography.

"There is no one hundred per cent guarantee in crypto."

# 54. New viable means of storing information for quantum technologies?

by CNRS
https://www.sciencedaily.com/releases/2021/08/210803084916.htm

In a study published on 3 August 2021 in *Physical Review X*, an international research team consisting of CNRS researcher Fabio Pistolesi and two foreign researchers used theoretical calculations to show that it is possible to realize a new type of qubit, in which information is stored in the oscillation amplitude of a carbon nanotube. These nanotubes can perform a large number of oscillations without diminishing, which shows their low level of interaction with the environment, and makes them excellent potential qubits. This property would enable for greater reliability in quantum computation.

A problem nevertheless persists with regard to the reading and writing of information stored in the first two energy levels of these oscillators. Scientists successfully proved that this information could be read by using the coupling between electrons, a negatively charged particle, and the flexural mode of these nanotubes.

This changes the spacing between the first levels of energy enough to make them accessible independently from other levels, thereby making it possible to read the information they contain. These promising theoretical predictions have not yet been verified experimentally.

# 55. Emerging technology, evolving threats — Part I: Quantum computing

by John McClurg
https://www.securitymagazine.com/articles/95765-emerging-technology-evolving-threats-part-i-quantum-computing

As technology grows and advances, potential cyber threats grow with it. While this notion is nothing new, the current speed of innovation makes it more important than ever to consider the implications these developments will have on our cybersecurity capabilities — especially with cybercriminals becoming more sophisticated and more adept at using emerging blind spots to their advantage.

Cybercriminals are already finding new ways to hack existing systems — increasingly targeting physical entities like critical infrastructure — and too often we are finding ourselves reacting to the situation, attempting to mitigate damages after the fact. We simply need to be better prepared. And while that is far easier said than done, what we can do — right now — is stay as informed and as educated as possible on the implications of these giant technological leaps. These advancements will undoubtedly accelerate the rate at which we see cyber threats emerge, making cybercriminals potentially even more dangerous.

In this first part of my "Emerging Tech, Evolving Threats" series, we will initiate an exploration of a technology that is simultaneously pushing society forward and opening new doors for cyberattacks.

## Quantum Computing

Traditional computers and computing systems operate on binary bits — information processed in the form of ones or zeroes. Quantum computing, on the other hand, transmits information via quantum bits, or qubits, which can exist either as a one or zero or both simultaneously. So rather than having to perform tasks sequentially like a traditional computer, quantum computers can run vast numbers of parallel computations. But what does that mean in terms of manifestable power? In 2019, Google resolved a calculation on a quantum computer in just minutes that would have taken a classical computer more than 10,000 years to complete.

Fortunately, the ubiquitous presence of such power yet lies a way off, which suggests we should have time to prepare ourselves. Many people think that quantum computing most likely will not be realized in the near term. In fact, John Donohue, scientific manager at the University of Waterloo's Institute for Quantum Computing, notes "the [quantum computing] community is pretty comfortable saying that's not something that's going to happen in the next five to 10 years."

## Cybersecurity Implications

Here is why that projected timeline is so important. The practical implications of such technology may not become fully clear or appreciated until it arrives. Notwithstanding that, some of its game-changing implications are already fully grasped. The cybersecurity world must, consequently, start preparing now. NIST is one organization that already is grappling with the implications of the fact that one of the most widely used schemes for safely transmitting data is poised to become obsolete once quantum computing reaches a sufficiently advanced state.

The cryptography systems that provide the safety architecture for a plethora of privacy protocols supporting everything from retail transactions to email communications, have relied on the fact that the computing power required to explore every possible way to decrypt your data was not heretofore available. A quantum computer, however, could attempt every possible decryption option in a matter of hours.

As previously mentioned, all new technological leaps come accompanied with corresponding new threats — and that has created quite the conundrum. While cryptography professionals scramble to gain more time and information with which to secure our data from quantum computers, pursuit of the technology's numerous potential upsides is not slowing — from drug discoveries to biological engineering to financial modeling.

While other the industries will be drastically changed and will benefit from the introduction of quantum computing, cybersecurity stands poised to be entirely upended. In the past months, we've seen the damage hackers can cause using AI and machine learning to carry out various types of malware and, more recently, ransomware attacks to cripple critical infrastructure. Threat actors can leverage the strengths of quantum computing to create novel approaches to breaching current cybersecurity practices.

It's important that the cybersecurity community act now in order to sufficiently defend against the potential threat that comes with quantum computing. While it might strike some as premature to start building a defense against a threat or vulnerability potentially 10+ years away, it actually takes more than 10 years to replace the existing and widely used web standards. It is, therefore, vital to explore and address potential quantum attack vectors now, instead of waiting until the emergence of general-purpose and commercial quantum computers.

If done properly, the quantum computing technological leap can bring about enormous, cross-industry change benefiting the lives of millions. If overlooked or underestimated, the cyber vulnerabilities it brings with it could bring consequences the likes of which have never been seen before. More on these challenges in my next column.

# 56. Quantum computing's next big challenge: A quantum skills shortage

by Daphne Leprince-Ringuet
https://www.zdnet.com/article/quantum-computings-next-challenge-finding-quantum-developers-and-fast/

System architects, software engineers, data analysts -- at first glance, the jobs that are hot in the quantum computing sector don't sound all that different from the tech roles we're already familiar with. Which deal with the classical computers we know well, from smartphones to supercomputers.

But to fill the burgeoning opportunities in quantum, transferring even the most expert knowledge of classical computers into the quantum world just won't cut it.

Quantum computers are fundamentally different from the classical devices we know and use every day. Instead of relying on bits, quantum systems leverage the complex laws of quantum physics to create quantum bits, or 'qubits', that are capable of carrying out calculations exponentially faster.

Building, programming and maintaining a quantum computer, therefore, is a radically different paradigm. It requires an understanding of quantum physics and how to map problems to the quantum space -- think programming languages, architectures, workflows and software, all of which are specific to quantum computing.

And it turns out that finding workers who have that breadth of knowledge is becoming more and more difficult.

"Finding someone with the right skill mix is the biggest challenge," Ross Duncan, the head of quantum software at Cambridge Quantum, tells *ZDNet*. "It's happened only a handful of times among the people that we hired to get someone who was ready to start when they walked in the door."

As a company focusing on creating quantum software, Cambridge Quantum usually looks for candidates who both grasp theoretical quantum computing while also being competent software developers.

"It's putting together a physics background with a computing background and trying to find candidates who have both," says Duncan. And that's not the most typical combination on a CV.

The issue isn't restricted to quantum software businesses. A company working on quantum superconducting hardware, for example, is likely to need someone that can build the infrastructure that cools down the system's processor -- which requires knowledge and expertise not only in quantum physics and cryogenics but also computer science skills to carry out testing and trialling.

In other words, employers need quantum employees with interdisciplinary skills: on top of a background in quantum physics, some sort of experience with data analysis, engineering, modelling or programming, among other things, will also be a must-have.

## Wanted: quantum doctors

That level of specialisation isn't common; in fact, it mostly exists at the PhD level. And the problem is, there aren't enough PhD graduates.

"If you're trying to hire for quantum skills, you end up having to look for very interdisciplinary training, and what you end up needing is usually PhDs," Abe Asfaw, quantum education lead at IBM, tells *ZDNet*. "The rate at which PhDs is being generated is far slower than the industry needs today, so we're seeing very intense competition to hire new PhDs in the field."

Of course, for now, the quantum computing industry is still something of a niche. This is largely because the technology is nascent: with most quantum computers currently supporting about 100 qubits or less, there's very little that can actually be done with the existing systems.

As a result, only a few companies are investing in the space, and the number of quantum roles, while growing, remains relatively low. But this is expected to change as businesses increasingly show interest in quantum technologies. Some estimates predict that the quantum computing industry will be a $65 billion market by 2030; others anticipate that up to 20% of organizations could be budgeting for quantum computing in 2023, up from 1% in 2018.

With a larger industry comes more demand for qualified workers -- but PhD-level quantum candidates aren't produced overnight.

"As a guess, I'd say there are probably a couple of dozen of PhD students produced in the UK each year that specialise in topics that are relevant to what we are doing, and I could hire them all myself," says Duncan. "In the short term, the constraints are going to become worse because we don't have the capacity to spin up a whole new lot of PhD programs."

The long-term solution is pretty obvious: education programs need to be reformed to bring the level of interdisciplinarity required by businesses down to the undergraduate level.

This is something that experts from both industry and academia have been considering for a number of years. In 2019, a symposium of 50 quantum experts from the US and Europe gathered at the University of California to discuss the issue and drafted a report looking at the current state of Quantum Information Science and Engineering (QISE) education programs. One of the main shortcomings that were highlighted in the report was the lack of alignment between higher education degrees and industry requirements.

For a company like Cambridge Quantum, those requirements are mostly technical. Duncan also mentions the possibility of online learning and professional training while new tools are emerging, such as IBM's first quantum developer certification, to help learners get up to scratch.

But beyond the need for employees who know how to build and manipulate a quantum computer, the industry is now also expanding to include organisations that are not quantum by nature but nevertheless interested in finding out what the technology could do to improve their business model.

There too, explains Ivan Ostojic, partner at tech consultancy McKinsey, some talent gaps are lurking, and they will need to be filled.

"At the moment, a lot of businesses are experimenting with quantum computing to see how they can extract value or valuable learnings," Ostojic tells *ZDNet*. "They will need what we call business translators, who need to have a deep understanding of the business and of the type of problems they are trying to solve that can't be answered with classical computers."

"At the same time, they will need to be fluent in quantum technologies, know what quantum systems are in development and how mature they are. Companies will need people who know both sides of the equation, business and quantum."

Understanding how quantum could boost efficiencies for banks is likely to require a candidate with some knowledge of finance. A materials design company looking at quantum computers might need a chemist. A basic knowledge of particle physics is useful to know whether quantum technologies could help discover the fundamental laws of nature.

This gap could also be solved at the university level, in the form of double majors combining quantum with a specialism -- but companies will likely have to take it upon themselves to develop talent early to make sure that employees understand their specific business problems, and how they can be answered with quantum computing.

Some of the more forward-thinking companies seem to have understood what is at stake. For example, banking giant JP Morgan, which has long been researching the potential of quantum computers for finance applications, created a summer associate program designed as an internship for students enrolled in a master's or PhD degree.

The requirements for the job include a degree in computer science, maths, engineering or sciences, as well as experience with quantum computing algorithms and applications; and successful candidates are promised the opportunity to collaborate on research to develop quantum solutions to problems faced by internal teams.

One of the most alluring benefits featuring on the job ad? Top-performing candidates can expect a full-time offer at the firm.

For giants like JP Morgan, the strategy is likely to pay off. With experts trained from an early stage to know how quantum computing can be tailored to the company's needs, the firm is setting itself for future success.

For smaller companies, however, competing for quantum talent could become an existential issue. Itamar Sivan, the CEO of Quantum Machines, explains that the challenge is already more tangible. "A few years back, it was easy to hire everywhere," Sivan tells *ZDNet*. "But the field is now transitioning from academia to industry, and as the industry grows, academia can't keep up.

"In countries like the US, where there are all the multinationals and a ton of start-ups, everyone is shoving their heads into the same pool of talents," he continues.

Looking for quantum candidates in the US is now difficult, continues Sivan, who doesn't expect the situation to ease over the next few years.

And with businesses set to be fighting over quantum-qualified job seekers in the near future, now might be the right time to start studying.

# 57. Quantum computers: China has ambitious plans

by Djoomart Otorbaev
https://news.cgtn.com/news/2021-08-02/Quantum-computers-China-has-ambitious-plans-12oN4j4xWUM/index.html

In three papers published on arXiv.org on June 28 and 29, scientists from the University of Science and Technology of China (USTC) reported fundamental advances in quantum communications and quantum computing.

In one, researchers used nanometer-sized semiconductors called quantum dots to transmit single photons over 300 kilometers of fiber. This result was more than 100 times better than all previous attempts.

In another, scientists improved their photonic quantum computer from 76 detected photons to 113, which significantly increased its "quantum advantage." It shows how much faster it is than traditional computers at one specific task.

The third paper presented the Zu Chongzhi quantum computer, consisting of 66 superconducting qubits. It used 56 of them to solve a particular problem, which exceeded the computational speed achieved by 53-qubit computers applied by Google Sycamore and set a performance record in 2019 .

"It's an exciting development. I did not know that they were coming out with not one but two of these [quantum computing results] in the same week," says Scott Aaronson, a theoretical computer scientist at the University of Texas at Austin. "That's pretty insane."

All three achievements are leading globally, but the experts are especially excited about Zu Chongzhi because this is the first confirmation and a significant excess of Google's Sycamore landmark result in 2019. "I'm very pleased that someone has reproduced the experiment and shown that it works properly," says John Martinis, a former Google researcher who led the effort to build Sycamore.

This year begins implementing China's 14th Five-Year Plan, which sets goals and strategies for the country's economic development until 2025. The plan resulted from joint action with the government's official political advisory body, the Chinese People's Political Consultative Conference (CPPCC). Renowned Chinese quantum physicist Pan Jianwei, a member of the CPPCC, said that the plan includes "major national scientific and technological projects in frontier fields including quantum information technology."

As part of this document, by the end of the 14th Five-Year Plan, it is planned to develop quantum computers with more than a few hundred qubits.

In December 2020, a research team led by Pan Jianwei announced another significant computing breakthrough, achieving quantum computational advantage. Scientists have created a new quantum computer, Jiuzhang, which computes 10 billion times faster than Google's Sycamore prototype. Compared to conventional computers, Jiuzhang is "a champion in a single field," according to the research team. Still, its super computing capabilities have enormous potential in graph theory, machine learning, and quantum chemistry. The breakthrough resulted from 20 years of effort by Pan's team, which conquered several major technological stumbling blocks, including a high-quality photon source.

There have been few other outstanding results in the field of quantum computing. In one example, a Chinese startup has announced plans to sell a quantum desktop computer for less than $5,000. The new handheld device is part of the SpinQ line and will be designed even for schools and colleges. Shenzhen SpinQ Technology will manufacture it. It was not the company's first quantum computer. Last year, it began selling a desktop quantum computer for about $50,000. The first sample was quite big and weighed 55kg, but the new machine will be simpler, more portable, and cheaper.

Unprecedented competition is unfolding in this area. China is leading the way with a quantum program worth at least $10 billion over the next five years, of which $3 billion will go into quantum computing.

The U.S. House of Representatives passed the $1.275 billion National Quantum Initiative Act, complementing ongoing initiatives by the Department of Energy, the Office of Army Research, and the National Science Foundation.

The European Union has allocated $1.1 billion, and the UK $381 million in additional funding for quantum technology. Many other countries, especially Australia, Canada and Israel, are also very active.

Back in 2017, a group of Chinese scientists emitted entangled photons from the national satellite Micius to conduct the world's first quantum security video call. American experts immediately sounded the alarm that China had suddenly become a leader in the critical area of quantum communications.

In response, American politicians decided urgently to invest hundreds of millions of dollars in the development of quantum informatics through the National Quantum Initiative.

The current situation is reminiscent of what had developed in 1957 when the U.S. similarly launched an unprecedented development program for its space program in the wake of panic over a small Soviet satellite called Sputnik. Will Americans be able to repeat their leap for quantum advantage this time?