Crypto News

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

August 01, 2021

Table des matières

1. Foreword

SEATTLE, WA – August, 1st, 2021. The Cloud Security Alliance (CSA) , the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment, today released the Crypto News compiled by Dhananjoy Dey member of the CSA Quantum-Safe Security Working Group (QSS WG). The CSA QSS WG was formed to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting their networks and their data. Individuals interested in joining the working group and participating in future research can do so by visiting the page at https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/ or the LinkedIn account.

The Crypto News is intended to provide an overview of the latest news in quantum-safe security and more broadly in security.

About Cloud Security Alliance.
The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem. For further information, visit us at https://cloudsecurityalliance.org/, and follow us on Twitter @cloudsa.

2. Quantum computers: The future on its way

by Djoomart Otorbaev
https://news.cgtn.com/news/2021-07-31/Quantum-computers-The-future-on-its-way-12jGFL8IVsk/index.html

Quantum computing is heating up as a growing number of entities race to benchmark and commercializes this technology. On June 28, the ArXiv magazine published an article, which reported the creation by Chinese scientists of a superconducting quantum computer named **Zuchongzhi**, which they called the most powerful in the world. The two-dimensional quantum computer consisted of 66 qubits, and the scientists used 56 qubits to solve the problem of sampling the output distribution of random quantum computer circuits. According to the developers, the computer coped with this task in just 1.2 hours, while the most modern computers would have taken eight years to complete this task.

It is now clear that quantum computing technology is rapidly gaining momentum. And it is becoming evident that quantum processors can solve various tasks billions of times faster than most modern computers. A Boston Consulting Group (BCG) report states that quantum computing could "change the game in such fields as cryptography and chemistry (and thus material science, agriculture, and pharmaceuticals) not to mention artificial intelligence and machine learning, logistics, manufacturing, finance, and energy." Many companies such as Visa, JPMorgan Chase, and Volkswagen are actively experimenting with quantum technologies even at the current early stage of their development.

Goldman Sachs recently announced that they plan to implement quantum algorithms for pricing financial instruments within five years. High-tech companies such as Google, IBM, Intel, and Honeywell have started to invest heavily in new technologies and are trying hard to commercialize them. In 2019, Google declared Sycamore quantum computer with a 53-qubit processor was able to solve a problem that a regular computer could handle in ten thousand years. In June 2020, Honeywell created a 64-qubit quantum processor. Intel has installed a quantum processor on a silicon chip, and the IBM quantum processor cloud platform is getting available to developers and programmers.

Chirag Dekate, vice president of technology research firm Gartner, believes that public cloud providers such as Amazon, Microsoft, and Google actively invest in next-generation quantum computing. They find it increasingly challenging to achieve performance gains with traditional chips. Gartner estimates that by 2025, nearly 40 percent of large companies are expected to be ready to embrace quantum computing actively. According to Research and Markets, another research firm, the global quantum computing hardware market will surpass $7.1 billion by 2026.

A recent BCG study found that the quantum computing sector received $1.15 billion in investment in 2018-2020, nearly double the amount in all prior years. However, in 20 years, the new industry will create up to $850 billion in value. Honeywell gives an even more optimistic outlook. They predict that the quantum industry will reach $1 trillion in turnover in the coming decades.

The fundamental change over the past two years has been explosive interest and investments from commercial corporations, according to BCG business unit chief Matt Langione. "This was the last element in the domino effect after governments and private equity investors began to invest heavily," he said. The report notes that quantum computing contributes to solving four fundamental problems: simulation, optimization, machine learning, and cryptography. Soon, the effect in pharmaceuticals will be up to $ 80 billion a year, in encryption for the needs of government agencies - up to $ 80 billion, in optimization of logistics networks - up to $ 100 billion, in search and advertising optimization - up to $ 100 billion, in the development of chemical catalysts - up to $ 50 billion, in the optimization of financial portfolios - up to $ 50 billion, in the prevention of money laundering and fraud - up to $ 30 billion.

In its July 14 article in Nature, Google claimed that its Sycamore quantum computer could detect and correct computational errors, an essential step for large-scale quantum computing. Julian Kelly of Google AI Quantum said that this progress means that the company will soon be able to create practical and reliable quantum computers. "This is basically our first half step along the path to demonstrating that. A viable way of getting to really large-scale, error-tolerant computers. It's sort of a look ahead for the devices that we want to make in the future."

Google plans to spend several billion dollars building a quantum computer by 2029 that can perform large-scale commercial and scientific calculations, said Hartmut Neven, a distinguished Google scientist who oversees the Quantum AI program. The company recently opened an expanded California-based campus, focusing on these efforts. For real industrial applications of quantum processors, Google said, a 1-million-qubit machine would need to be built to perform reliable, error-free computations.

Dario Gil, director of IBM Research, recently said that 2023 would be a watershed moment in that the errors of quantum computers will continue to decrease exponentially with software, not just hardware.

Perhaps it can be argued that now there is no longer any doubt that scientists and engineers will soon create commercial quantum computers. The companies and countries are betting big on this technology. The question is, who will get it first. But in any case, unique opportunities in the latest developments and newest discoveries will open up before humanity quite soon.

3. Preparing for the Post-Quantum Migration: A Race to Save the Internet

by Nicholas Acevedo
https://www.jdsupra.com/legalnews/preparing-for-the-post-quantum-2468064/

Most people don't know, or care to know, about cryptography. Without cryptography, the internet privacy that we all rely on for transmitting virtually all forms of digital communication would be insecure from attackers. Our current encryption methods are threatened by the breakthrough in quantum computing. Unless proactive steps are taken to mitigate this threat, large-scale quantum computers will tear down the backbone of the internet, secure communications.

Cryptography is the "process of securing data in transit or stored by third party adversaries."[1] Cryptographic schemes encrypt data, rendering it into an unreadable math equation of ones and zeros that is relatively easy to unravel with a key, but are difficult for an adversary to reverse engineer. The majority of crypto-systems rely on asymmetric cryptography (public-private keys) and symmetric cryptography (public-public key). Both types of cryptography require the sender of information to encrypt the data with a public key. These cryptographic methods establish private and secure communication channels over the internet, seamlessly occurring every second going largely unnoticed. Current technology is based on difficult math problems that today's computers can't easily resolve. Through the use of hard to solve algorithms, modern cryptography methods have encrypted our data in a way that was initially expected to take thousands, if not millions, of years to crack on conventional computers.

According to many leading experts, large-scale quantum computers are predicted to arrive in the next ten years, rendering the "unbreakable" cryptographic methods relied on for modern encryption decipherable in less than a day.[2] Quantum computers utilize the laws of quantum mechanics, enabling them to solve certain classes of complex calculations much faster than conventional computers.

To put this into real terms: to break a 2,048-bit encryption used today a conventional computer would need about 300 trillion years, a quantum computer with 4,099 qubits would take 10 seconds.

Although modern encryption remains "unbreakable" until the development of large-scale quantum computers, digital communications must be secured against quantum computers long before their creation. IBM plans to have a 1,000 qubit quantum computer by 2023 and, although we don't think IBM will use the technology to break competi-

[1] Vasileios Mavroeidies et al., *The Impact of Quantum Computing on Present Cryptography*, 9 IJACSA 1, 1 (Mar. 31, 2018).

[2] Quantum computing has been on Gartner's list of emerging technologies repeatedly over the years. This 2019 article estimated 5 to 10 years before consistent results are achieved, allowing for the commercialization of quantum computing. https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing/

tors' encryption, security experts warn of the risk posed by a "capture now, exploit later" attack.[3] In this form of attack, encrypted data may be recorded or stolen today and stored by adversaries until quantum computers provide the capabilities needed to break the asymmetric algorithm and decrypt the data at a later date.

National agencies and scientific institutions are well aware of the threat of quantum computers to existing cryptography. In 2015, the United States National Security Agency first published warnings of the need to transition to quantum-resistant algorithms. One year later, the National Institute of Standards and Technology ("NIST") began a standardization initiative for post-quantum cryptography and secure operating parameters. Post-quantum cryptography is the study of crypto-systems that can be run on a conventional computer and is sufficiently secure against both quantum and conventional computers. However, the trial process is lengthy and NIST continues to review and scrutinize potential quantum-resistant algorithms. The initiative identified five classes of cryptographic systems that are currently quantum-resistant: lattice based; multivariate-quadratic-equations; hash-based; code-based; and supersingular elliptic curve isogeny. NIST is expected to announce the first algorithm to qualify for standardization within the next two years.

During this transition period while the world awaits NIST's findings, there are measures that can be taken now to begin securing data against quantum computing and preparing for the upcoming migration. Organizations should begin the engineering work necessary to prepare their infrastructure for the implementation of post-quantum cryptography as soon as the migration is ready. To begin preparing now, experts recommend that organizations create a reference index for those applications that use encryption and ensure that current and future systems have sufficient cryptographic agility. Reference indexing allows organizations to assess quantum vulnerabilities ensuring that all applications are migrated, minimizing the risk of incidents occurring in one part of their digital ecosystem. It is essential that organizations perform an ongoing assessment of their risks and migrate quickly to prevent systemic data insecurity.
Organizations should develop a plan to transition to quantum-resistant encryption. Planning ahead will minimize system down time and provide flexibility for responding to any implementation flaws. Organizations can utilize their reference index to ensure that all of their hardware is capable of utilizing quantum-resistant encryption. The migration process will require complicated planning and budgeting, but by beginning to prepare now for the upcoming migration to post-quantum cryptography, organizations can ensure a less disruptive transition.

In addition, to protect data from potential "**capture now, exploit later**" attacks, enterprises can begin implementing a hybrid approach to encryption by using both classical and post-quantum schemes together. Migrating applications to quantum-resistant encryption quickly is the only proactive step organizations can take to mitigate this risk. If an organization implements hybrid encryption, it is essential to remain aware of NIST findings in case the chosen quantum-resistant algorithm is found to be breakable. Moreover, the implemented post-quantum encryption may need to be updated in order to align with NIST secure operating parameters.

As the race continues to protect the internet from the threat of exploitation using quantum computers, it is essential that organizations prepare themselves today for the complexities involved in a global migration to post-quantum cryptographic algorithms. The security of today's digital information depends on it.

4. Eternal Change for No Energy: A Time Crystal Finally Made Real

[3] Campagna M., LaMacchia B., & Ott D. (2020) Post Quantum Cryptography: Readiness Challenges and the Approaching Storm. https://cra.org/ccc/resources/ccc-led-whitepapers/#2020-quadrennial-papers

by Natalie Wolchover
https://www.quantamagazine.org/first-time-crystal-built-using-googles-quantum-computer-20210730/

In a preprint posted online Thursday night, researchers at Google in collaboration with physicists at Stanford, Princeton and other universities say that they have used Google's quantum computer to demonstrate a genuine "time crystal." In addition, a separate research group claimed earlier this month to have created a time crystal in a diamond.

A novel phase of matter that physicists have strived to realize for many years, a time crystal is an object whose parts move in a regular, repeating cycle, sustaining this constant change without burning any energy.

"The consequence is amazing: You evade the second law of thermodynamics," said Roderich Moessner, director of the Max Planck Institute for the Physics of Complex Systems in Dresden, Germany, and a co-author on the Google paper. That's the law that says disorder always increases.

Time crystals are also the first objects to spontaneously break "time-translation symmetry," the usual rule that a stable object will remain the same throughout time. A time crystal is both stable and ever-changing, with special moments that come at periodic intervals in time.

The time crystal is a new category of phases of matter, expanding the definition of what a phase is. All other known phases, like water or ice, are in thermal equilibrium: Their constituent atoms have settled into the state with the lowest energy permitted by the ambient temperature, and their properties don't change with time. The time crystal is the first "out-of-equilibrium" phase: It has order and perfect stability despite being in an excited and evolving state.

"This is just this completely new and exciting space that we're working in now," said Vedika Khemani, a condensed matter physicist now at Stanford who co-discovered the novel phase while she was a graduate student and co-authored the new paper with the Google team.

Khemani, Moessner, Shivaji Sondhi of Princeton and Achilleas Lazarides of Loughborough University in the United Kingdom discovered the possibility of the phase and described its key properties in 2015; a rival group of physicists led by Chetan Nayak of Microsoft Station Q and the University of California, Santa Barbara identified it as a time crystal soon after.

Researchers have raced to create a time crystal over the past five years, but previous demos, though successful on their own terms, have failed to satisfy all the criteria needed to establish the time crystal's existence. "There are good reasons to think that none of those experiments completely succeeded, and a quantum computer like [Google's] would be particularly well placed to do much better than those earlier experiments," said John Chalker, a condensed matter physicist at the University of Oxford who wasn't involved in the new work.

Google's quantum computing team made headlines in 2019 when they performed the first-ever computation that ordinary computers weren't thought to be able to do in a practical amount of time. Yet that task was contrived to show a speedup and was of no inherent interest. The new time crystal demo marks one of the first times a quantum computer has found gainful employment.

"It's a fantastic use of [Google's] processor," Nayak said.

With yesterday's preprint, which has been submitted for publication, and other recent results, researchers have fulfilled the original hope for quantum computers. In his 1982 paper proposing the devices, the physicist Richard Feynman argued that they could be used to simulate the particles of any imaginable quantum system.

A time crystal exemplifies that vision. It's a quantum object that nature itself probably never creates, given its complex combination of delicate ingredients. Imaginations conjured the recipe, stirred by nature's most baffling laws.

5. What is quantum computing? Everything you need to know about the strange world of quantum computers

by Daphne Leprince-Ringuet
https://www.zdnet.com/article/what-is-quantum-computing-everything-you-need-to-know-about-the-strange-world-of-quantum-computers/

Quantum computing exploits the puzzling behavior that scientists have been observing for decades in nature's smallest particles – think atoms, photons or electrons. At this scale, the classical laws of physics ceases to apply, and instead we shift to quantum rules.

While researchers don't understand everything about the quantum world, what they do know is that quantum particles hold immense potential, in particular to hold and process large amounts of information. Successfully bringing those particles under control in a quantum computer could trigger an explosion of compute power that would phenomenally advance innovation in many fields that require complex calculations, like drug discovery, climate modelling, financial optimization or logistics.

As Bob Sutor, chief quantum exponent at IBM, puts it: "Quantum computing is our way of emulating nature to solve extraordinarily difficult problems and make them tractable," he tells ZDNet.

What is a quantum computer?

Quantum computers come in various shapes and forms, but they are all built on the same principle: they host a quantum processor where quantum particles can be isolated for engineers to manipulate.

The nature of those quantum particles, as well as the method employed to control them, varies from one quantum computing approach to another. Some methods require the processor to be cooled down to freezing temperatures, others to play with quantum particles using lasers – but share the goal of finding out how to best exploit the value of quantum physics.

What's the difference between a quantum computer and a classical computer?

The systems we have been using since the 1940s in various shapes and forms – laptops, smartphones, cloud servers, supercomputers – are known as classical computers. Those are based on bits, a unit of information that powers every computation that happens in the device.

In a classical computer, each bit can take on either a value of one or zero to represent and transmit the information that is used to carry out computations. Using bits, developers can write programs, which are sets of instructions that are read and executed by the computer.

Classical computers have been indispensable tools in the last few decades, but the inflexibility of bits is limiting. As an analogy, if tasked with looking for a needle in a haystack, a classical computer would have to be programmed to look through every single piece of hay straw until it reached the needle.

There are still many large problems, therefore, that classical devices can't solve. "There are calculations that could be done on a classical system, but they might take millions of years or use more computer memory that exists in total on Earth," says Sutor. "These problems are intractable today."

How do quantum computers improve on classical devices?

At the heart of any quantum computer are qubits, also known as quantum bits, and which can loosely be compared to the bits that process information in classical computers.

Qubits, however, have very different properties to bits, because they are made of the quantum particles found in nature – those same particles that have been obsessing scientists for many years.

One of the properties of quantum particles that is most useful for quantum computing is known as superposition, which allows quantum particles to exist in several states at the same time. The best way to imagine superposition is to compare it to tossing a coin: instead of being heads or tails, quantum particles are the coin while it is still spinning.

By controlling quantum particles, researchers can load them with data to create qubits – and thanks to superposition, a single qubit doesn't have to be either a one or a zero, but can be both at the same time. In other words, while a classical bit can only be heads or tails, a qubit can be, at once, heads and tails.

This means that, when asked to solve a problem, a quantum computer can use qubits to run several calculations at once to find an answer, exploring many different avenues in parallel.

So in the needle-in-a-haystack scenario about, unlike a classical machine, a quantum computer could in principle browse through all hay straws at the same time, finding the needle in a matter of seconds rather than looking for years – even centuries – before it found what it was searching for.

What's more: qubits can be physically linked together thanks to another quantum property called entanglement, meaning that with every qubit that is added to a system, the device's capabilities increase exponentially – where adding more bits only generates linear improvement.

Every time we use another qubit in a quantum computer, we double the amount of information and processing ability available for solving problems. So by the time we get to 275 qubits, we can compute with more pieces of information than there are atoms in the observable universe. And the compression of computing time that this could generate could have big implications in many use cases.

Why is quantum computing so important?

"There are a number of cases where time is money. Being able to do things more quickly will have a material impact in business," Scott Buchholz, managing director at Deloitte Consulting, tells ZDNet.

The gains in time that researchers are anticipating as a result of quantum computing are not of the order of hours or even days. We're rather talking about potentially being capable of calculating, in just a few minutes, the answer to problems that today's most powerful supercomputers couldn't resolve in thousands of years, ranging from modelling hurricanes all the way to cracking the cryptography keys protecting the most sensitive government secrets.

And businesses have a lot to gain, too. According to recent research by Boston Consulting Group (BCG), the advances that quantum computing will enable could create value of up to $850 billion in the next 15 to 30 years, $5 to $10 billion of which will be generated in the next five years if key vendors deliver on the technology as they have promised.

What is a quantum computers used for?

Programmers write problems in the form of algorithms for classical computers to resolve – and similarly, quantum computers will carry out calculations based on quantum algorithms. Researchers have already identified that some quantum algorithms would be particularly suited to the enhanced capabilities of quantum computers.

For example, quantum systems could tackle optimization algorithms, which help identify the best solution among many feasible options, and could be applied in a wide range of scenarios ranging from supply chain administration to traffic management. ExxonMobil and IBM, for instance, are working together to find quantum algorithms that could one day manage the 50,000 merchant ships crossing the oceans each day to deliver goods, to reduce the distance and time traveled by fleets.

Quantum simulation algorithms are also expected to deliver unprecedented results, as qubits enable researchers to handle the simulation and prediction of complex interactions between molecules in larger systems, which could lead to faster breakthroughs in fields like materials science and drug discovery.

With quantum computers capable of handling and processing much larger datasets, AI and machine learning applications are set to benefit hugely, with faster training times and more capable algorithms. And researchers have also demonstrated that quantum algorithms have the potential to crack traditional cryptography keys, which for now are too mathematically difficult for classical computers to break.

What are the different types of quantum computers?

To create qubits, which are the building blocks of quantum computers, scientists have to find and manipulate the smallest particles of nature – tiny parts of the universe that can be found thanks to different mediums. This is why there are currently many types of quantum processors being developed by a range of companies.

One of the most advanced approaches consists of using superconducting qubits, which are made of electrons, and come in the form of the familiar chandelier-like quantum computers. Both IBM and Google have developed superconducting processors.

Another approach that is gaining momentum is trapped ions, which Honeywell and IonQ are leading the way on, and in which qubits are housed in arrays of ions that are trapped in electric fields and then controlled with lasers.

Major companies like Xanadu and PsiQuantum, for their part, are investing in yet another method that relies on quantum particles of light, called photons, to encode data and create qubits. Qubits can also be created out of silicon spin qubits – which Intel is focusing on – but also cold atoms or even diamonds.

Quantum annealing, an approach that was chosen by D-Wave, is a different category of computing altogether. It doesn't rely on the same paradigm as other quantum processors, known as the gate model. Quantum annealing processors are much easier to control and operate, which is why D-Wave has already developed devices that can manipulate thousands of qubits, where virtually every other quantum hardware company is working with about 100 qubits or less. On the other hand, the annealing approach is only suitable for a specific set of optimization problems, which limits its capabilities.

What can you do with a quantum computer today?

Right now, with a mere 100 qubits the state of the art, there is very little that can actually be done with quantum computers. For qubits to start carrying out meaningful calculations, they will have to be counted in the thousands, and even millions.

"While there is a tremendous amount of promise and excitement about what quantum computers can do one day, I think what they can do today is relatively underwhelming," says Buchholz.

Increasing the qubit count in gate-model processors, however, is incredibly challenging. This is because keeping the particles that make up qubits in their quantum state is difficult – a little bit like trying to keep a coin spinning without falling on one side or the other, except much harder.

Keeping qubits spinning requires isolating them from any environmental disturbance that might cause them to lose their quantum state. Google and IBM, for example, do this by placing their superconducting processors in temperatures that are colder than outer space, which in turn require sophisticated cryogenic technologies that are currently near-impossible to scale up.

In addition, the instability of qubits means that they are unreliable, and still likely to cause computation errors. This has given rise to a branch of quantum computing dedicated to developing error-correction methods.

Although research is advancing at pace, therefore, quantum computers are for now stuck in what is known as the NISQ era: noisy, intermediate-scale quantum computing – but the end-goal is to build a fault-tolerant, universal quantum computer.

As Buchholz explains, it is hard to tell when this is likely to happen. "I would guess we are a handful of years from production use cases, but the real challenge is that this is a little like trying to predict research breakthroughs," he says. "It's hard to put a timeline on genius."

What is quantum supremacy?

In 2019, Google claimed that its 54-qubit superconducting processor called Sycamore had achieved quantum supremacy – the point at which a quantum computer can solve a computational task that is impossible to run on a classical device in any realistic amount of time.

Google said that Sycamore has calculated, in only 200 seconds, the answer to a problem that would have taken the world's biggest supercomputers 10,000 years to complete.

More recently, researchers from the University of Science and Technology of China claimed a similar breakthrough, saying that their quantum processor had taken 200 seconds to achieve a task that would have taken 600 million years to complete with classical devices.

This is far from saying that either of those quantum computers are now capable of outstripping any classical computer at any task. In both cases, the devices were programmed to run very specific problems, with little usefulness aside from proving that they could compute the task significantly faster than classical systems.

Without a higher qubit count and better error correction, proving quantum supremacy for useful problems is still some way off.

What is the use of quantum computers now?

Organizations that are investing in quantum resources see this as the preparation stage: their scientists are doing the groundwork to be ready for the day that a universal and fault-tolerant quantum computer is ready.

In practice, this means that they are trying to discover the quantum algorithms that are most likely to show an advantage over classical algorithms once they can be run on large-scale quantum systems. To do so, researchers typically try to prove that quantum algorithms perform comparably to classical ones on very small use cases, and theorize that as quantum hardware improves, and the size of the problem can be grown, the quantum approach will inevitably show some significant speed-ups.

For example, scientists at Japanese steel manufacturer Nippon Steel recently came up with a quantum optimization algorithm that could compete against its classical counterpart for a small problem that was run on a 10-qubit quantum computer. In principle, this means that the same algorithm equipped with thousands or millions of error-corrected qubits could eventually optimize the company's entire supply chain, complete with the management of dozens of raw materials, processes and tight deadlines, generating huge cost savings.

The work that quantum scientists are carrying out for businesses is therefore highly experimental, and so far there are fewer than 100 quantum algorithms that have been shown to compete against their classical equivalents – which only points to how emergent the field still is.

Who is going to win the quantum computing race?

With most use cases requiring a fully error-corrected quantum computer, just who will deliver one first is the question on everyone's lips in the quantum industry, and it is impossible to know the exact answer.

All quantum hardware companies are keen to stress that their approach will be the first one to crack the quantum revolution, making it even harder to discern noise from reality. "The challenge at the moment is that it's like looking at a group of toddlers in a playground and trying to figure out which one of them is going to win the Nobel Prize," says Buchholz.

"I have seen the smartest people in the field say they're not really sure which one of these is the right answer. There are more than half a dozen different competing technologies and it's still not clear which one will wind up being the best, or if there will be a best one," he continues.

In general, experts agree that the technology will not reach its full potential until after 2030. The next five years, however, may start bringing some early use cases as error correction improves and qubit counts start reaching numbers that allow for small problems to be programmed.

IBM is one of the rare companies that has committed to a specific quantum roadmap, which defines the ultimate objective of realizing a million-qubit quantum computer. In the nearer-term, Big Blue anticipates that it will release a 1,121-qubit system in 2023, which might mark the start of the first experimentations with real-world use cases.

What about quantum software?

Developing quantum hardware is a huge part of the challenge, and arguably the most significant bottleneck in the ecosystem. But even a universal fault-tolerant quantum computer would be of little use without the matching quantum software.

"Of course, none of these online facilities are much use without knowing how to 'speak' quantum," Andrew Fearnside, senior associate specializing in quantum technologies at intellectual property firm Mewburn Ellis, tells ZDNet.

Creating quantum algorithms is not as easy as taking a classical algorithm and adapting it to the quantum world. Quantum computing, rather, requires a brand-new programming paradigm that can only be ran on a brand-new software stack.

Of course, some hardware providers also develop software tools, the most established of which is IBM's open-source quantum software development kit Qiskit. But on top of that, the quantum ecosystem is expanding to include companies dedicated exclusively to creating quantum software. Familiar names include Zapata, QC Ware or 1QBit, which all specialize in providing businesses with the tools to understand the language of quantum.

And increasingly, promising partnerships are forming to bring together different parts of the ecosystem. For example, the recent alliance between Honeywell, which is building trapped ions quantum computers, and quantum software company Cambridge Quantum Computing (CQC), has got analysts predicting that a new player could be taking a lead in the quantum race.

What is cloud quantum computing?

The complexity of building a quantum computer – think ultra-high vacuum chambers, cryogenic control systems and other exotic quantum instruments – means that the vast majority of quantum systems are currently firmly sitting in lab environments, rather than being sent out to customers' data centers.

To let users access the devices to start running their experiments, therefore, quantum companies have launched commercial quantum computing cloud services, making the technology accessible to a wider range of customers.

The four largest providers of public cloud computing services currently offer access to quantum computers on their platform. IBM and Google have both put their own quantum processors on the cloud, while Microsoft's Azure Quantum and AWS's Braket service let customers access computers from third-party quantum hardware providers.

What does the quantum computing industry look like today?

The jury remains out on which technology will win the race, if any at all, but one thing is for certain: the quantum computing industry is developing fast, and investors are generously funding the ecosystem. Equity investments in quantum computing nearly tripled in 2020, and according to BCG, they are set to rise even more in 2021 to reach $800 million.

Government investment is even more significant: the US has unlocked $1.2 billion for quantum information science over the next five years, while the EU announced a €1 billion ($1.20 billion) quantum flagship. The UK also recently reached the £1 billion ($1.37 billion) budget milestone for quantum technologies, and while official numbers are not known in China, the government has made no secret of its desire to aggressively compete in the quantum race.

This has caused the quantum ecosystem to flourish over the past years, with new start-ups increasing from a handful in 2013 to nearly 200 in 2020. The appeal of quantum computing is also increasing among potential customers: according to analysis firm Gartner, while only 1% of companies were budgeting for quantum in 2018, 20% are expected to do so by 2023.

Who is getting quantum-ready now?

Although not all businesses need to be preparing themselves to keep up with quantum-ready competitors, there are some industries where quantum algorithms are expected to generate huge value, and where leading companies are already getting ready.

Goldman Sachs and JP Morgan are two examples of financial behemoths investing in quantum computing. That's because in banking, quantum optimization algorithms could give a boost to portfolio optimization, by better picking which stocks to buy and sell for maximum return.

In pharmaceuticals, where the drug discovery process is on average a $2 billion, ten-year-long deal that largely relies on trial and error, quantum simulation algorithms are also expected to make waves. This is also the case in materials science: companies like OTI Lumionics, for example, are exploring the use of quantum computers to design more efficient OLED displays.

Leading automotive companies including Volkswagen and BMW are also keeping a close eye on the technology, which could impact the sector in various ways, ranging from designing more efficient batteries to optimizing the supply chain, through to better management of traffic and mobility. Volkswagen, for example, pioneered the use of a quantum algorithm that optimized bus routes in real time by dodging traffic bottlenecks.

As the technology matures, however, it is unlikely that quantum computing will be limited to a select few. Rather, analysts anticipate that virtually all industries have the potential to benefit from the computational speedup that qubits will unlock.

Will quantum computers replace our laptops?

Quantum computers are expected to be phenomenal at solving a certain class of problems, but that doesn't mean that they will be a better tool than classical computers for every single application. Particularly, quantum systems aren't a good fit for fundamental computations like arithmetic, or for executing commands.

"Quantum computers are great constraint optimizers, but that's not what you need to run Microsoft Excel or Office," says Buchholz. "That's what classical technology is for: for doing lots of maths, calculations and sequential operations."

In other words, there will always be a place for the way that we compute today. It is unlikely, for example, that you will be streaming a Netflix series on a quantum computer anytime soon. Rather, the two technologies will be used in conjunction, with quantum computers being called for only where they can dramatically accelerate a specific calculation.

How will we use quantum computers?

Buchholz predicts that, as classical and quantum computing start working alongside each other, access will look like a configuration option. Data scientists currently have a choice of using CPUs or GPUs when running their workloads, and it might be that quantum processing units (QPUs) join the list at some point. It will be up to researchers to decide which configuration to choose, based on the nature of their computation.

Although the precise way that users will access quantum computing in the future remains to be defined, one thing is certain: they are unlikely to be required to understand the fundamental laws of quantum computing in order to use the technology.

"People get confused because the way we lead into quantum computing is by talking about technical details," says Buchholz. "But you don't need to understand how your cellphone works to use it."

"People sometimes forget that when you log into a server somewhere, you have no idea what physical location the server is in or even if it exists physically at all anymore. The important question really becomes what it is going to look like to access it."

And as fascinating as qubits, superposition, entanglement and other quantum phenomena might be, for most of us this will come as welcome news.

6. Cybersecurity Performance Goals for Critical Infrastructure Operators

by Mariam Baksh
https://www.defenseone.com/policy/2021/07/white-house-asks-cisa-nist-set-cyber-security-performance-goals-critical-infrastructure-operators/184104/

The White House will issue a national security memo Wednesday instructing the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology to establish cybersecurity performance goals for private-sector owners and operators of critical infrastructure.

The goal is to set comprehensive expectations for cybersecurity across all sectors of critical infrastructure at a time when private companies might be more inclined to meet them, a senior administration official told reporters Tuesday.

The official said the administration expects the action will make a difference even though it’s not a requirement because of “the fact that it's being announced by the president in the context of the [Transportation Security Administration’s] recent mandate, in the context of us openly saying that we really are committed to addressing the limited and piecemeal regulation, in the context of the current environment where the threat is known and seen by critical infrastructure owners and private sectors.”

“You look at a Colonial Pipeline, you look at JBS foods, you look at Kaseya, there is now a different threat,” said the official, listing victims of recent ransomware attacks with reverberating effects. “The threats that many people talked about have become real. So we believe these goals will be viewed differently.”

7. IBM Unveils Japan’s First Commercial Quantum Computer

by Matt Swayne
https://thequantumdaily.com/2021/07/27/ibm-unveils-japans-first-commercial-quantum-computer/

With news of a quantum computer installation in Japan, IBM is earning a gold medal for establishing international collaborations for quantum computing.
The The University of Tokyo will use the IBM Quantum System One, an integrated quantum computer system, to drive quantum research and development in Japan, namely in the areas of chemistry, optimization, and machine learning. IBM now has installed IBM Quantum System Ones on three continents.

This is the company's latest step in a long and growing relationship with quantum researchers in Japan. In a blog post, the company reports that they launched a hub at Keio University in 2018. The University of Tokyo and IBM kicked off the Japan-IBM Quantum Partnership in 2019.

They write: "As part of this partnership, researchers in Japan will receive an IBM Quantum System One, to be installed at the Kawasaki Business Incubation Center at Kawasaki City. The aim of this partnership is to engage universities in Japan to accelerate quantum computing research and education, work with industry to advance research in practical quantum computing applications, and to develop commercial quantum computing hardware components."

This installation is the latest example of momentum in a growing quantum industry, the company reports.

"Whether or not quantum computing will make a difference is no longer in question. Instead, the question is how and when will the industry reach the pivotal milestone of Quantum Advantage – the point in which a quantum computer can solve a problem faster than a classical computer."

8. APPLICATIONS AND USE CASES OF QUANTUM COMPUTING IN TODAY'S WORLD

by Satavisa Pati
https://www.analyticsinsight.net/applications-and-use-cases-of-quantum-computing-in-todays-world/

Quantum computing is the latest way to a smarter version of AI. The unprecedented power of quantum computers makes them useful in many scenarios where classical computers would require an impractical amount of time to solve a problem. For example, they could simulate quantum systems, allowing scientists to study in detail the interactions between atoms and molecules. This, in turn, could help in the design of new materials (e.g., electronics, chemical materials) or new medicines. As they are significantly faster than classical computers, quantum computers will also be far more efficient at searching through a space of potential solutions for the best solution to a given problem. Quantum computers rely on quantum bits – qubits – to process information; in doing so, they use two key quantum mechanical properties: superposition and entanglement. Superposition is the ability of a quantum system to be in multiple states at the same time. Qubits still use the binary 0 and 1 system, but the superposition property allows them to represent a 0, a 1, or both at the same time. Instead of analyzing 0s and 1s sequence by sequence, two qubits in superposition can represent four scenarios at the same time, thus reducing the time needed to process a data set. Quantum computers can thus pave the way for unparalleled innovations in medicine and healthcare, allowing for the discovery of new medications to save lives or of new AI methods to diagnose diseases. They can also support the

discovery of new materials, the development of enhanced cybersecurity methods, the elaboration of much more efficient traffic control and weather forecasting systems, and more.

Use Cases of Quantum Computing

Airbus has launched a quantum computing challenge to encourage the development of quantum solutions in aircraft climb and loading optimization, as well as wing box design optimization. Daimler is working with Google on using quantum computing in the fields of materials science and quantum chemical simulation. The US Department of Energy is funding research projects that could lead to the development of very sensitive sensors (with applications in medicine, national security, and science) and provide insights into cosmic phenomena such as dark matter and black holes. Google, IBM, Intel, Microsoft, and other major tech companies are allocating significant resources to quantum computing research, in their efforts to pioneer breakthroughs in areas such as AI and machine learning, medicine, materials, chemistry, supply chains, and logistics, financial services, astrophysics, and others.

Use of Quantum in Cryptography

Quantum cryptography is a method used for the secured, encrypted transfer of information. Unlike other forms of cryptography, it ensures security by the laws of physics; it is not dependent on mathematical algorithms and does not secure exchanges of keys. Quantum communication based on quantum cryptography currently qualifies as highly secure, making it impossible to wiretap or intercept. Here, the most well-known application is quantum key distribution (QKD), which relies on the use of quantum mechanical effects to perform cryptographic tasks.

Quantum Teleportation

One possible means of quantum communication is quantum teleportation. Although the name can be misleading, quantum teleportation is not a form of the transport of physical objects but a form of communication. This teleportation is the process of transporting a qubit from one location to another without having to transport the physical particle to which that qubit is attached. Even quantum teleportation depends on the traditional communication network, making it impossible to exceed the speed of light.

Use of Quantum Computing in Workplace

In January 2019, IBM announced its first commercial quantum computer that can work outside the research lab, but with a power of only 20 qubits. Later on, in October 2019, the company's engineers announced the development of a 53-qubit computer. The start-up Rigetti Computing developed a 32-qubit computer and is now working on a 128-qubit one too. In October 2019, Google claimed that it achieved 'quantum supremacy' with a 53-qubit quantum computing chip that took 200 seconds to carry out a specific calculation which would have taken a classical computer 10 000 years to complete. IBM soon challenged that claim, arguing that the problem solved by Google's computer could also be solved in just 2.5 days through a different classical technique.

9. PsiQuantum Closes $450 Million Funding Round to Build the World's First Commercially Viable Quantum Computer

by Julien-Levallois
https://www.swissquantumhub.com/psiquantum-closes-450-million-funding-round-to-build-the-worlds-first-commercially-viable-quantum-computer/

PsiQuantum has raised $450 million in Series D funding to build the world's first commercially viable quantum computer. The funding round was led by funds and accounts managed by BlackRock, along with participation from insiders including Baillie Gifford and M12 – Microsoft's venture fund – and new investors including Blackbird Ventures and Temasek. PsiQuantum has now raised a total of $665 million in funding to date.

PsiQuantum was founded in 2016 by the world's foremost quantum computing experts, who understood that a useful quantum computer required fault-tolerance and error correction, and therefore at least 1 million physical qubits. The company includes a growing team of world-class engineers and scientists who are working on the entire quantum computing stack, from the photonic and electronic chips, through packaging and control electronics, cryogenic systems, quantum architecture and fault tolerance, to quantum applications. In May 2020, the company started manufacturing the silicon photonic and electronic chips that form the foundation of the Q1 system, a significant system milestone in PsiQuantum's roadmap to deliver a fault-tolerant quantum computer.

Quantum computing is anticipated to unlock the solutions to otherwise impossible problems, enabling extraordinary advances across a broad range of applications including climate, energy, healthcare, finance, agriculture, transportation, materials design, and more.

"Quantum computing is the most profoundly world-changing technology uncovered to date," said Jeremy O'Brien, CEO and co-founder of PsiQuantum. "It is my conviction that the way to bring this technology into reality is by using photonics. Our company was founded on the understanding that leveraging semiconductor manufacturing is the only way to deliver the million qubits that are known to be required for error correction, a prerequisite for commercially valuable quantum computing applications. This funding round is a major vote of confidence for that approach."

Unlike other quantum computing efforts, PsiQuantum is exclusively focused on building a fault-tolerant quantum computer supported by a scalable and proven manufacturing process. The company has developed a unique technology in which single photons (particles of light) are manipulated using photonic circuits which are patterned onto a silicon chip using standard semiconductor manufacturing processes. PsiQuantum is manufacturing quantum photonic chips, as well as the cryogenic electronic chips to control the qubits, using the advanced semiconductor tools in the production line of PsiQuantum's manufacturing partner GlobalFoundries.

"A commercially viable, general-purpose quantum computer has the potential to create entirely new industries ready to address some the most urgent challenges we face, especially in climate, healthcare, and energy," said Tony Kim, managing director at BlackRock. "To see this promising technology deployed within a reasonable time frame requires it to be built using a scalable manufacturing process. Silicon photonics combined with an advanced quantum architecture is the most promising approach we've seen to date."

"Investing is about backing companies with the potential to deliver transformational growth," said Luke Ward, investment manager at Baillie Gifford. "With its uniquely scalable approach, PsiQuantum is on track to deliver the world's first useful quantum computer and unlock a powerful new era of innovation in the process. Whether it's developing better battery materials, improving carbon capture techniques, or designing life-saving drugs in a fraction of the time, quantum computing is key to solving many of the world's most demanding challenges."

"We invested in PsiQuantum based on the strength of the company's bold vision matched by a robust, disciplined, stepwise engineering plan to achieve that goal," said Samir Kumar, managing director at Microsoft's venture fund M12. "We are impressed by the technical progress we have seen in hardware development along with refinement of

a novel quantum architecture ideally suited for photonics. PsiQuantum and Microsoft have a shared perspective on the need for a good number of logical qubits enabled by fault tolerance and error correction on 1 million-plus physical qubits, when it comes to building a truly useful quantum computer."

When fault-tolerant quantum computers become available, humankind will be able to use them to solve otherwise impossible problems. PsiQuantum is currently working with global leaders in the healthcare, materials, electronics, financial, security, transportation, and energy sectors to identify and optimize algorithms and applications to support business readiness for the broad adoption of quantum computing.

10.The Great Quantum Computing Race

by MARK LAPEDUS

https://semiengineering.com/the-great-quantum-computing-race/

Quantum computing is heating up, as a growing number of entities race to benchmark, stabilize, and ultimately commercialize this technology.

As of July 2021, a group from China appears to have taken the lead in terms of raw performance, but Google, IBM, Intel and other quantum computer developers aren't far behind. All of that could change overnight, though. At this point, it's too early to declare a winner in quantum computing, a technology that promises to outperform today's conventional supercomputers.

Today, Google, IBM and others have built the first wave of quantum computers, but these systems are still in the early stages and aren't yet running any useful commercial applications — yet. Nevertheless, there is noticeable progress with quantum computing, which is different than today's systems.

In today's computing, the information is stored in bits, which can be either a "0" or "1". In quantum computing, the information is stored in quantum bits, or qubits, which can exist as a "0" or "1" or a combination of both. The superposition state enables a quantum computer to perform multiple calculations at once, enabling it to outperform a traditional system. But the technology faces a number of challenges, and many industry experts believe these systems are still a decade away from being practical.

However, that's not stopping companies, governments, R&D organizations and universities from developing the technology and pouring billions of dollars into the arena. If they are realized, quantum computers could accelerate the development of new chemistries, drugs and materials. The systems also could crack any encryption, which has made their development a top priority among several nations. And across the board, it could provide companies and countries with a competitive edge.

"Quantum computing is at the forefront of national initiatives," said Amy Leong, senior vice president at FormFactor. "There have been more than $20 billion in investments announced across 15 countries here. Geopolitical powerhouses like the U.S. and China are certainly leading the race to claim quantum supremacy, followed by a host of others from Europe and Asia."

The race is heating up among nations as well as between different organizations. In a major development, the University of Science and Technology of China (USTC) in June 2021 demonstrated what researchers claim is the world's fastest quantum computing processor, surpassing the previous and unofficial record held by Google's 53-qubit device since 2019. USTC's 66-qubit processor performed a complex calculation in 1.2 hours that would have taken today's supercomputers 8 years to complete.

Google, IBM, Intel and other quantum computing developers aren't standing still, and are aggressively devising faster processors. It's too early to declare a winner, as the technology is still in its infancy. "When I take a look at the first applications, we're going to need several thousand, if not 100,000 qubits, to do something useful," said James Clarke, director of quantum hardware at Intel. "If we're at 50 to 60 qubits today, it's going to be a while before we can get to 100,000 qubits. It's going to be awhile before we can get to 1 million qubits, which would be necessary for cryptography."

Meanwhile, there is another race within this race. Vendors are developing a dozen types of qubits based on a range of technologies, such as ion trap, silicon spin and superconductivity. Vendors from each camp claim their technology is superior, and will enable practical quantum computers. It's too early to declare a technology winner here, as well.

Still, the market is promising. The quantum computer market is projected to grow from $320 million in 2020 to $830 million by 2024, according to Hyperion Research.

Classical vs. quantum computing

Viewed as a timeline, the computing field has made enormous progress. In 1945, the University of Pennsylvania developed ENIAC, the first general-purpose electronic digital computer. Using vacuum tubes to process the data, ENIAC executed 5,000 additions per second. Vacuum tubes are used to control electrons.

The advent of the transistor in 1947 changed everything. Starting in the 1950s, transistors replaced vacuum tubes in many systems, and enabled faster computers.

Meanwhile, in 1964, now-defunct Control Data introduced the CDC 6600, the world's first supercomputer. Based on transistors, the 6600 incorporated a 60-bit processor with 2 MIPS of performance.

Fast forward to today, and the smart phone is faster than the early computers. Apple's iPhone 12 incorporates the A14 processor based on TSMC's 5nm process. Incorporating 11.8 billion transistors, the A14 features a 6-core CPU and a 16-core neural engine capable of 11 trillion operations per second.

At the high end, Fugaku in 2021 retained its position as the world's fastest supercomputer. Built by Riken and Fujitsu, Fugaku is based on Arm's A64FX processor. It has 7,630,848 cores, enabling 442 petaflops per second of performance. A petaflop performs one quadrillion floating-point operations per second.

Fugaku is in operation and is being used for various research projects. "(Fugaku) embodies technologies realized for the first time in a major server general-purpose CPU, such as 7nm process technology, on-package integrated HBM2, terabyte-class streaming capabilities and an on-die embedded high-performance network," said Satoshi Matsuoka, director of the Center for Computational Science at Riken, in a paper at the 2021 Symposia on VLSI Technology and Circuits.

"We are well into the petaflop computing era," said Aki Fujimura, CEO of D2S. "There are many research computers around the globe that are approaching exascale computing (1,000 petaflops). We will have many exascale computers by the end of this decade."

Indeed, the industry requires more compute power to solve current and future problems in biotechnology, defense, materials science, medicine, physics, and weather prediction.

"We need to compute more at the same price. The problems are getting harder. The problems we serve are getting bigger and harder on top of that," Fujimura said.

While traditional computing will continue to progress, the industry is rushing to develop quantum computing. In theory, these new systems promise to outperform today's supercomputers, which could speed up the development of new technologies.

In the distant future, quantum computers are expected to be able to crack the world's most complex algorithms within a reasonable time. This includes Shor's algorithm, an integer factorization problem that can be utilized to break the widely used public-key cryptography scheme known as RSA.

Conceived in the 1980s, quantum computing has made some major strides over the years. Recently, two systems have achieved "quantum supremacy." This describes a point where quantum computers can do things that a classical computer can't.

Still, quantum computing is in its infancy. Work is underway to advance these systems, and find useful applications for the technology. "All systems that exist today are primarily used to explore future quantum applications, including looking at variational quantum algorithms for quantum chemistry, and quantum kernel estimation methods for machine learning," said Jerry Chow, director of quantum hardware system development at IBM. "The systems that are deployed today are also interesting from the standpoint of benchmarks and characterization of their own performance, and to understand underlying noise sources to improve future iterations of these systems. One other aspect is to explore the concept of quantum error correction."

Even if quantum computers realize their potential, they won't replace today's computers. "Quantum computing is clearly an important future technology for some types of computing problems. Prime factorization is another task that quantum computing is known to be far superior at than classical computing," D2S' Fujimura said. "In a way, quantum computing will augment classical computing for some specific difficult problems. On a larger scale, quantum computing will not replace classical computing. Classical computing is more appropriate for many of the tasks we need to compute."

Today's quantum computers are different and resemble giant chandeliers. These systems are housed in a dilution refrigerator capable of shielding the processor and other components from external noise and heat. The unit cools the devices between 10 and 15 milliKelvin.

A quantum system consists of a processor, which incorporates the qubits. Those qubits come in two configurations, with one-qubit and two-qubit gates. Let's say you have a quantum processor with 16 qubits. The qubits are arranged in a two-dimensional 4 X 4 array. The first three rows (top to bottom) may consist of one-qubit gates. The last row may have two-qubit gates.

The processing functions are complex. In classical computing, you put a number into the computer, it calculates the function, and gives you an output.

Let's say you have problem with 2^n bits of data. "If you have 'n' bits, you have 2^n. That's an exponentially large number of states, and you can only work on them one at a time. So, it's exponential time or exponential in space," explained William Oliver, a professor at the Massachusetts Institute of Technology (MIT), in a video presentation. "A quantum computer, on the other hand, can take those 2n different components and put them all into one superposition state simultaneously. And this is what underlies the exponential speed up that we see in a quantum computer."

There are other advantages. "In order to double the power of a quantum computer, you only have to add one qubit. It's exponential. In order for a quantum computer to keep up with a classical computer in terms of Moore's Law, they only have to add one qubit every 24 months," said Paul Smith-Goodson, an analyst at Moor Insights & Strategy.

This all works in theory. What prevents quantum computing from realizing its full potential are several major issues. First, qubits lose their properties, typically within 100 microseconds, due to noise, according to IBM.

That's why qubits must operate in extremely cold environments. "Qubits are extremely sensitive to their environment," FormFactor's Leong said. "Quieting down the qubit environment in a very cold or cryogenic environment is critical."

In addition, noise causes errors in the qubits. So quantum computers require error correction. On top of that, the industry needs to scale up quantum computers with thousands of qubits. It's nowhere close to that figure.

All told, quantum computing requires some breakthroughs. "We need to make qubits better than we're making them today. And that's across the field," Intel's Clarke said. "To me, the biggest challenge is how you wire them up. Every qubit requires its own wire and its control box. That works well when you have 50 or 60 qubits. It doesn't work well when you have a million of them."

Manufacturing qubits with good yields is also critical. Onto Innovation and others are developing metrology processes around the technology.

"Right now, we've conducted measurements on a few wafers or coupons," said Kevin Heidrich, senior vice president at Onto. "The key behind most of the foundational technologies in quantum is utilizing the manufacturing technologies developed for classical computing. However, many are tweaking the devices, designs and integrations to enable quantum/qubit devices. The key engagements we have are around enabling precise and characterized devices to enable various forms of quantum computing such as photonic or spin qubits. Our focus is to provide metrology solutions to enable our development partners to best characterize their early devices, including things like precise sidewall control, materials thickness, and interface quality."

Superconducting qubits

Today, there are 98 organizations working on quantum computers and/or qubits, according to the Quantum Computing Report. Companies are developing different types of qubits, including ion trap, neutral atoms, photonics, silicon spin, superconducting and topological. Each type is different, with some advantages and disadvantages. It's too early to say which technology is superior.

"We really don't know which technology is going to be the right technology to build a grand scheme fault tolerant machine. Companies have a five-year roadmap, leading to where they are going to have enough qubits to actually do something meaningful," said Smith-Goodson from Moor Insights & Strategy. "(Regarding the installed base), IBM has a large number of machines. They have over 20 quantum computers and no one can match that. They have a large ecosystem built up around it. They have a lot of universities and companies that they're working with."

So far, superconducting qubits have made the most progress. In this category, D-Wave has gained attention by using quantum annealing, a technology that solves optimization problems. For example, if you have a problem with many combinations, a quantum annealing system searches for the best of many possible combinations. These capabilities have been demonstrated, at least to some degree.

Most of the activity is taking place in the bonafide quantum computer market using supercomputing qubits. Google, IBM, Intel, MIT, Rigetti, USTC and many others are developing products here.

Superconducting qubits are built around Josephson junctions. A Josephson junction includes a thin insulating layer, which is sandwiched by two superconducting metals. In operation, electrons pair up and tunnel through the junction.

In 2014, IBM demonstrated a 3-qubit device. Today, IBM sells a quantum computer with 65 qubits. Until recently, IBM led the industry in terms of overall qubit count in the superconducting space, according to the Quantum Computing Report. At present, the unofficial record is held by USTC with 66 qubits. IBM is next with 65, followed by Google with 53 qubits, Intel (49) and Rigetti (32), according to the Quantum Computing Report.

Qubit count isn't the only factor. They also must have relatively long coherence times and gate fidelities. "Qubits and quantum processors are the central part of quantum hardware," IBM's Chow said. "To build a quantum computer or a quantum computing system, we will need not only quantum hardware, but also control electronics, classical computing units, and software that runs quantum computing programs."

On that front, IBM offers Qiskit, an open-source quantum software development kit. "Our goal is to have a broad engagement of the developer community and grow a quantum ecosystem to bring quantum computers to users as their essential tools in their research and business," Chow said.

The industry also will require systems with thousands of qubits, but vendors have a long way to go here. The results are still promising, however. In 2019, Google's 53-qubit processor, called Sycamore, completed a calculation in 200 seconds. Google claimed it would take a supercomputer about 10,000 years to finish the same task.

Then, in June of 2021, China's USTC presented a paper on Zuchongzhi, a 66-qubit superconducting quantum processor. In a calculation, USTC utilized 56 qubits. It performed a task 2 to 3 times faster than Google's 53-qubit processor. "We expect this large-scale, high-performance quantum processor could enable us to pursue valuable quantum applications beyond classical computers in the near future," said Jian-Wei Pan, a professor of USTC, in a paper. Others contributed to the work.

The results from China and elsewhere are up for debate. Many don't use any benchmarks to report their results, including quantum volume, which is a metric to express the effectiveness of a quantum computer. "It all doesn't depend on qubits. We don't know how many of these systems perform. If you don't have error correction and get up to a certain point, you can add all the qubit you want to and it's never going to be any more powerful," said Smith-Goodson from Moor Insights & Strategy.

Meanwhile, besides USTC's processor, there are other developments in superconducting qubits:

Rigetti introduced a multi-chip quantum processor, enabling an 80-qubit system by year's end.

By year's end, IBM will release Eagle, a 127-qubit quantum processor. IBM is working on a 433-qubit processor for 2022, and a 1,121-qubit device for 2023.

Google found a way to reduce qubit error rates. It also plans to develop a 1 million qubit processor by 2029.

Ion traps

Ion trap qubits are another promising technology. With ion trap, atoms are at the heart of the quantum processor. The atoms are trapped, and then lasers do everything from the initial preparation to final readout, according to IonQ, a developer of the technology.

In ion trap, IonQ is leading with 32 qubits, followed by AQT (24), Honeywell (10) and others, according to the Quantum Computing Report.

On the R&D front, Sandia National Laboratories is developing QSCOUT, a quantum computer testbed based on ion trap qubits. QSCOUT is a 3-qubit system. Sandia plans to expand the system to 32 qubits over time.

With QSCOUT, Sandia is offering an open-access program for end-users. “Not only can users specify which gates (each circuit is made up of many gates) they want to apply and when, but they can also specify how the gate itself is implemented, as there are many ways to achieve the same result. These tools allow users to get into the weeds of the how the quantum computer works in practice to help us figure out the best way to build a better one,” said Susan Clark, a physicist and the QSCOUT lead at Sandia.

“Since we are a testbed system, the code running on our machine is generated by users, who have lots of ideas of what they might like to run on a quantum computer,” Clark said. “Thirty-two qubits are still small enough that it can be fully simulated on a classical computer, so the point is not to do something that a classical computer cannot do. The main reasons for building the smaller system are: 1) study how to map problems onto a quantum computer the best way for best performance on a future larger system (quantum chemistry, quantum system simulations), and 2) learn techniques for making a quantum computer run better that can be applied to a bigger machine.”

Like the superconducting qubit market, ion trap is also seeing a wave of activity. Honeywell, for example, is spinning off its quantum computing unit and will merge it with Cambridge Quantum Computing. Honeywell also demonstrated the ability to correct quantum errors in real time.

IonQ’s customers, meanwhile, can purchase access to its quantum computers via Google’s cloud services.

Silicon qubits

Silicon spin qubits are also promising. Leti, Intel, Imec and others are working on this technology. Intel appears to be leading with 26 qubits, according to the Quantum Computing Report.

“What we’re doing here is making a single electron transistor,” Intel’s Clarke said. “We’re making a transistor that has one electron in the channel. That single electron can either have spin up or spin down. That spin up or spin down represents the ‘0’ and the ‘1’.”

The trick is to make the electron move into the superposition state. “When you have one spin, it’s one qubit,” Clarke said. “If you have two electrons close to each other, or two of these spin qubits, then you can start to perform operations. You can start using quantum entanglement.”

Silicon spin qubits have some advantages. “Intel’s spin qubits are a million times smaller than some of the other qubit technologies,” Clarke said. “We’re going to need 100,000 to 1 million of them. When I envision what a quantum chip will look like in the future, it will look similar to one of our processors.”

In addition, spin qubits leverage some of the same processes and tools used in semiconductor fabs. The processes don’t involve leading-edge nodes. “A lot of our innovation comes more from the materials that we’re using rather than the patterning capability,” Clarke said.

There is a frenetic among of activity in silicon spin:

- Intel rolled out Horse Ridge II, a second-generation cryogenic control chip. The device brings control functions for quantum computer operations into the cryogenic refrigerator, which can streamline the complexity of the control wiring for quantum systems.
-
- CEA-Leti has developed an interposer that enables the integration of devices for quantum computing. The interposer connects qubits and control chips.
-
- Imec devised uniform spin qubit devices with tunable coupling in a 300mm integrated process.
-

- Intel and FormFactor have separately developed cryoprobers. These systems characterize qubits at cryogenic temperatures.

Conclusion

There are other types of qubits, as well. “You have photonics. People are using light particles and that looks like a promising field,” said Smith-Goodson from Moor Insights & Strategy.

But it’s unclear which technologies will prevail over time. The same is true for companies in this space.

Perhaps a bigger question is whether quantum computing will ever live up to the hype. But companies and countries are betting big on this technology. And given the progress so far, the current results and activity make this all worth watching.

11.Quantum entanglement-as-a-service: “The key technology” for unbreakable networks

by Esther Shein
https://www.techrepublic.com/article/quantum-entanglement-as-a-service-the-key-technology-for-unbreakable-networks/

Fueled by several recent contracts from the U.S. Air Force valued at up to $100,000, quantum networking company Aliro Quantum is advancing its efforts to develop quantum entanglement-as-a-service. The goal is to enable the distribution of entangled quantum states between nodes.

Quantum EaaS connects users of quantum networks with entangled quantum bits known as qubits, securely, across long distances.

Aliro's software control plane and simulation technology provide the foundation for enabling EaaS on today's quantum networks, the company said. Aliro calls EaaS "the key technology for the un-hackable secure networks of today and the quantum internet of tomorrow.”

Like classical networks, quantum networks require hardware-independent control plane software to manage data exchange between layers, allocate resources and control synchronization, the company said.

"We want to be the Switzerland of quantum networking," said Jim Ricotta, Aliro CEO.

Networked quantum computers are needed to run quantum applications such as physics-based secure communications and distributed quantum computing.

"A unified control plane is one of several foundational technologies that Aliro is focused on as the first networking company of the quantum era," Ricotta said. "Receiving Air Force contracts to advance this core technology validates our approach and helps accelerate the time to market for this and other technologies needed to realize the potential of quantum communication.”

How EaaS works

Entanglement is a physical phenomenon that involves tiny things such as individual photons or electrons, Ricotta said. When they are entangled, "then they become highly correlated" and appear together. It doesn't matter if they are hundreds of miles apart, he said.

"If you entangle two photons and someone makes a change to photon A, another person can observe that change at photon B, because they've been entangled," he explained. "It's the law of physics. But it's invisible to the naked eye."

Quantum networks work by entangling photons with information that can be encoded and then teleported over the same telecom fiber in the ground used today, Ricotta said. Entanglement enables the teleportation of qubits, which carry quantum information securely.

"To do useful work, you have to create thousands of entangled photon pairs per second because the entangled photons are the equivalent of bandwidth on a classical network," he said. "If we have thousands, or eventually tens of thousands per second, we can transfer lots of information."

There will be apps built on the quantum network that we can't envision yet, Ricotta said, but they are going to consume bandwidth--just like today's apps do on a classical network. The apps built for a quantum network will consume entanglement, meaning they will consume lots of pairs of entangled photons/qubits, he said.

Physics-based security versus quantum key distribution

Another approach to securely transferring encryption keys between two locations is Quantum key distribution. Although the keys are transferred using quantum physics, QKD typically does not use entanglement, according to Ricotta.

"The big problem with QKD is you build a network and you can only do key distribution for classical bits" in a single purpose network, he said. "We believe … if you go to the trouble of building a quantum network, just like today's internet, [you] will want to build many apps on it and have that flexibility."

A quantum network based on EaaS is a general-purpose network, whereas the network built for QKD can only be used to distribute those encryption keys, he said.

"That's some of the reason QKD hasn't caught on—it isn't really used much," Ricotta said, adding that the National Security Agency has said it doesn't believe QKD is a good idea.

"We think it makes more sense to build a general-purpose quantum network," he said.

For example, secure communications can be done using qubit teleportation on an EaaS network with the same software that is used on an EaaS network in a data center to connect several quantum computers to form a cluster. By networking together 10 50-qubit computers, your application gets access to 500 qubits. This is important, Ricotta said, because with more qubits, quantum computers can solve larger problems.

"When you talk to users of quantum computers,"such as drugs, finance and materials companies, "they say 'We can get value from quantum computers, but we need several hundred or a thousand qubits to run our algorithms.'"

12.Remote Employees Adopt Bad Cybersecurity Habits While Working from Home

by Stu Sjouwerman
https://blog.knowbe4.com/remote-employees-adopt-bad-cybersecurity-habits-while-working-from-home?utm_medium=email&_hsmi=143770266&_hsenc=p2ANqtz-_-aPZT7sBu1xEay-o4JKuOR7tmTmI2jtbffRWPAmf7_vPlywBWEqtwmJxo29QFXyFVDgGfT0-goNpljnABXwns6uIMWjA&utm_content=143770266&utm_source=hs_email

A new report focused on businesses looking to bring employees back to the office makes it very clear that security leaders are concerned, as remote workers have been anything but secure.

I don't entirely blame the remote worker – they were told to stay home, use the computer you own, start using these new web-based alternatives to work applications, figure out how to be productive, and somehow make it through the pandemic keeping their family and themselves safe. That's a lot to put on one person's plate… and then ask them to also be super vigilant and secure for the company's sake.

According to new data from security vendor Tessian in their Back to Work Security Behaviors Report, it's evident that security leaders are well aware of the challenges related to having tried to keep a remote workforce secure and how this is going to impact the business once employees come back to the office.

- 56% of IT leadership believe employees have adopted bad cybersecurity behaviors while working from home
- 54% are worried remote workers will bring infected devices and malware into the office

And employees are confirming this concern:

- 1 in 3 employees think they can get away with riskier security behaviors when working remotely
- 40% of employees plan to bring their personal device into the office to work on

So, we have an interesting juncture; IT leaders know less than secure users and devices are planning on coming back to the office. So, what are they to do? The device issue is easy enough to fix; only managed devices should be used (keeping in mind there are solutions that exist that can manage and secure personal devices out there). The employee issue is going to require Security Awareness Training to both educate users on why being vigilant is important, what good cybersecurity hygiene looks like, and how to identify social engineering attacks via email and the web.

13.Multiple encryption flaws uncovered in Telegram messaging protocol

by John Leyden
https://portswigger.net/daily-swig/multiple-encryption-flaws-uncovered-in-telegram-messaging-protocol

An analysis of the popular Telegram secure messaging protocol has identified four cryptographic vulnerabilities.

Although none of the flaws are particularly serious or easy to exploit, security researchers have nonetheless warned that the software “falls short on some essential data security guarantees”.

Standard deviation

Computer scientists from from ETH Zurich and Royal Holloway, University of London, uncovered the vulnerabilities after examining the open source code used to provide encryption services to the Telegram app. The audit excluded any attempt to attack any of Telegram’s live systems.

The researchers found that Telegram’s proprietary system falls short of the security guarantees enjoyed by other, widely deployed cryptographic protocols such as Transport Layer Security (TLS).

ETH Zurich professor Kenny Paterson commented that encryption services “could be done better, more securely, and in a more trustworthy manner with a standard approach to cryptography”.

The most significant vulnerability among the quartet makes it possible for an attacker to manipulate the sequencing of messages coming from a client to one of the cloud servers operate by Telegram.

A second flaw made it possible for an attacker on the network to detect which of two messages are encrypted by a client or a server, an issue more of interest to cryptographers than hostile parties, the researchers suggest.

The third security issue involves a potential manipulator-in-the-middle attack targeting initial key negotiation between the client and the server. This assault could only succeed after sending billions of messages.

A fourth security weakness made it possible (at least in theory) for an attacker to recover some plain text from encrypted messages – a timing-based side-channel attack that would require an attacker to send millions of messages and observe how long the responses take to be delivered. The researchers admit the attack is impractical while Telegram goes further and categorises it as a non-threat.

"The researchers did not discover a way to decipher messages," a representative of Telegram told *The Daily Swig*.

In a statement, the firm welcomed the research

> *The traits of MTProto pointed out by the group of researchers from the University of London and ETH Zurich were not critical, as they didn't allow anyone to decipher Telegram messages. That said, we welcome any research that helps make our protocol even more secure.*
>
> *These particular findings helped further improve the theoretical security of the protocol: the latest versions of official Telegram apps already contain the changes that make the four observations made by the researchers no longer relevant.*

The researchers notified Telegram about their research in April. Telegram has since patched all four flaws, clearing the way for researchers to go public with their findings through a detailed technical blog post.

TLS recommendation

Royal Holloway professor Martin Albrecht told *The Daily Swig* that the researchers offered lessons for other developers of secure messaging apps – for example, industry standard TLS encryption should be a preferred design choice.

"The 'mode' of Telegram we looked at was when messages are encrypted between the client and the server only," Albrecht explained.

"This is no different from running Facebook Messenger or IRC [Internet Relay Chat] over TLS. Here it makes little sense to not use TLS (or its UDP variants). It is well studied, including its implementations, it does not need special assumptions, it is less brittle than [for example] MTProto."

MTProto is the encryption scheme used by Telegram.

Telegram already relies on TLS for its security for messages from the server to Android clients, but it relies on proprietary approaches elsewhere.

Whether apps are built using TLS as a foundation or not, an audit by cryptographers is highly advisable.

Albrecht commented: "When we talk about secure messaging apps specifically, i.e messages are encrypted between the parties not just the transport layer between client and server, they should have cryptographers on staff who formally reason about the design. In the future this should get easier with the MLS standard."

Hong Kong Garden

The research into Telegram was motivated by use of technology by participants in large- scale protests such as those seen in 2019/2020 in Hong Kong.

"We found that protesters critically relied on Telegram to coordinate their activities, but that Telegram had not received a security check from cryptographers," according to Albrecht.

Albrecht was part of a team that researched what makes the Telegram platform attractive to high-risk users involved in mass protests, who are likely to be targeted by surveillance.

"Telegram does seem to have the advantage of 'staying up' in light of government crackdown in contrast to other social networks and seemingly not complying all that much with government requests," according to Albrecht.

Although mobile messaging apps such as Signal are often recommended and used by the security-savvy, features and utility are more important for mainstream users and go some way to explaining use of Telegram among protesters in Hong Kong and beyond.

"It might be better to compare Telegram to Facebook or Twitter (in terms of features and appeal) than to, say, Signal," he added.

Telegram may be preferred to Facebook even if the latter is likely better or at stricter when it comes to data governance, Albrecht concluded.

"On the flip side, it is not clear what security policies, processes and safeguards Telegram have in place to, e.g continuously vet their (server and client) code for software vulnerabilities, to prevent their own staff from snooping."

14.Variational quantum algorithm with information sharing

by Chris N. Self, Kiran E. Khosla, Alistair W. R. Smith, Frédéric Sauvage, Peter D. Haynes, Johannes Knolle, Florian Mintert & M. S. Kim
https://www.nature.com/articles/s41534-021-00452-9

We introduce an optimisation method for variational quantum algorithms and experimentally demonstrate a 100-fold improvement in efficiency compared to naive implementations. The effectiveness of our approach is shown by obtaining multi-dimensional energy surfaces for small molecules and a spin model. Our method solves related variational problems in parallel by exploiting the global nature of Bayesian optimisation and sharing information between different optimisers. Parallelisation makes our method ideally suited to the next generation of variational problems with many physical degrees of freedom. This addresses a key challenge in scaling-up quantum algorithms towards demonstrating quantum advantage for problems of real-world interest.

15.KT develops Q-SDN to monitor and control quantum cryptographic networks

by Lim Chang-won
https://www.ajudaily.com/view/20210722112101016

KT, a leading telecom company in South Korea, has developed a quantum-software defined network (Q-SDN) that can monitor and control quantum cryptographic networks from a central control center. It can link equipment from various manufacturers more easily if quantum cryptography networks are expanded.

Software-defined networking (SDN), which makes networks agile and flexible, is an approach to cloud computing that facilitates network management and enables programmatically efficient network configuration. Q-SDN optimizes quantum encryption key resource management and controls the transmission path of quantum encryption keys by monitoring and controlling quantum encryption communication networks from the center.

KT said that its Q-SDN technology adopted open interface standards to enhance compatibility between heterogeneous equipment. The technology would be applied to the establishment of a pilot quantum cryptography network.

KT applied automation technology and know-how of its network operation to control the quantum cryptography network, such as artificial intelligence hacking detection and automatic recovery for service stability and security. "We applied technology and experience gained from network automation to quantum cryptography networks so that quantum cryptography services can be used more conveniently and safely," KT's infrastructure research institute head Lee Jong-sik said in a statement on July 22.

16.Cambridge Quantum algorithm solves optimisation problems significantly faster, outperforming existing quantum methods

by Cambridge Quantum
https://cambridgequantum.com/cambridge-quantum-algorithm-solves-optimisation-problems-significantly-faster-outperforming-existing-quantum-methods/

In a development that is likely to set a new industry standard, scientists at Cambridge Quantum (CQ) have developed a new algorithm for solving combinatorial optimisation problems that are widespread in business and industry, such as travelling salesman, vehicle routing or job shop scheduling, using near-term quantum computers.

Mathematical conundrums like these lie at the heart of a vast range of real-world optimisation challenges such as designing manufacturing processes, filling delivery trucks or routing passenger jets. As the level of automation in modern global businesses increases year over year, optimisation algorithms running on even the most powerful classical computers are forced to trade accuracy for speed.

In this paper published on the pre-print repository arXiv, CQ scientists introduce the Filtering Variational Quantum Eigensolver (F-VQE) to make combinatorial optimisation more efficient. Using the Honeywell System Model H1 quantum computer, the new approach outperformed existing "gold standard" algorithms such as the Quantum Approximate Optimisation Algorithm (QAOA) and the original VQE, reaching a good solution 10 to 100 times faster.

The paper has been authored by CQ's research team comprising Michael Lubasch, Ph.D., David Amaro, Ph.D., Carlo Modica, Ph.D., Matthias Rosenkranz, Ph.D., and Marcello Benedetti, Ph.D.. The scientists are part of CQ's Machine Learning and Quantum Algorithms team headed by Dr. Mattia Fiorentini.

F-VQE leverages a method published in this paper by CQ in September 2020, which demonstrated how a quantum circuit can be decomposed into smaller circuits and run using fewer qubits without losing quantum advantage. As a result, a 23-qubit problem was solved by using only up to 6 hardware qubits at time. CQ's scientists also demonstrated that the new approach is highly adaptable for use with noisy intermediate-scale quantum (NISQ) era machines. These advancements increase the scale of the optimisation problems that are within reach of today's NISQ computers.

"Our scientists are honing in on a range of workable methods for today's quantum computers. We want enterprises and governments to achieve quantum advantage for general purpose tasks more quickly, and our experience of working with large industrial partners facilitates a deep understanding of the needs of practitioners today." said Fiorentini. "F-VQE has distinct advantages over previous quantum algorithms: it finds good candidate solutions faster and uses quantum hardware much more efficiently. F-VQE could have a transformative impact, helping to solve previously intractable problems across business and industry."

Ilyas Khan, CEO of CQ, said, “Our team of scientists is relentlessly focused on closing the gap between the real-world limits of classical computation and the quantum advantage that will be available in the NISQ era. They are establishing new standards in quantum computing and their research will inspire rapid further progress.”

Tony Uttley, President of Honeywell Quantum Solutions, said, “This project illustrates the exciting advances occurring in quantum computing. By developing algorithms that do more with fewer qubits and running them on the best hardware possible, we are making significant progress toward solving real-world problems sooner than expected.”

17.Researchers develop innovative platform capable of verifying quantum encryption technologies

by Lim Chang-won
https://www.ajudaily.com/view/20210721173811684

A state research body in South Korea has developed an innovative platform capable of verifying encryption technologies that prevent the hacking of quantum computers. It would accelerate efforts to find cryptographic algorithms with higher security in preparation for the era of quantum computers.

The Electronics and Telecommunications Research Institute (ETRI) said that the new platform called "Q Crypton," unveiled at an online conference on July 21, can verify the quantum safety of various cryptographic systems such as RSA, which is a public-key cryptosystem that is widely used for securing data transmission, and next-generation quantum-resistant passwords.

Q Crypton laid the foundation for verifying cryptographic algorithms and the performance of programs that will be used in quantum computers, ETRI said, adding the platform would be released step by step through a web browser to prevent hacking using quantum computers.

"The fear of incapacitating modern public key cryptography with quantum computers is coming to reality. Based on the world's best technology in cryptographic quantum safety, we will work hard to establish next-generation security infrastructure early," ETRI's cybersecurity research division head Kim Ik-kyun said in a statement on July 21.

Quantum cryptography is an essential security solution for safeguarding critical information. Data encoded in a quantum state is virtually unhackable without quantum keys which are basically random number tables used to decipher encrypted information. Binary digital electronic computers are based on transistors and capacitors with data encoded into binary digits (bits). Quantum computation uses quantum bits or qubits.

Q Crypton platform can analyze and simulate the quantitative safety of passwords more accurately as it can consider various factors such as different qubit sizes, quantum computer chip structures, and an error rate. Because the platform is equipped with visualization programming technology and a library of key computations for encryption, it is possible to develop quantum algorithms needed for encryption quickly and efficiently.

ETRI said the platform schematized quantum circuits so that numerous and complex formulas can be seen intuitively at a glance and shortened so that they are not inputted one by one. the platform provides the language processing

of quantum algorithms, verification using virtual machines, and a function to analyze the amount of quantum resources.

Post-quantum cryptography (PQC) refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer. Even though current, publicly known, experimental quantum computers lack the processing power to break any real cryptographic algorithm, many cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat.

18.Honeywell, Google bring practical quantum computers a big step closer

by Stephen Shankland
https://www-cnet-com.cdn.ampproject.org/c/s/www.cnet.com/google-amp/news/honeywell-google-bring-practical-quantum-computers-a-big-step-closer/

Honeywell and Google have detailed dueling demonstrations of logical qubits, a technology that can correct errors in potentially powerful but notoriously finicky quantum computers.

In a research paper released Wednesday, Honeywell said it had ganged together multiple physical qubits -- the storage and processing units of quantum computers -- so that they could withstand disturbances from outside forces like vibration and electromagnetic emissions.

The results arrived one week after Google published a paper in Nature Communications also showing logical qubits overpowering errors. Google's approach, however, didn't achieve full error correction: its method only could handle one of two error types at a time instead of both simultaneously, and it couldn't fix errors it detected. That's why Honeywell is claiming its full error correction achievement as a first.

"Big enterprise-level problems require precision and error-corrected logical qubits to scale successfully," said Tony Uttley, Honeywell Quantum Solutions' president, in a statement.

Honeywell's technique marks a significant step in the development of quantum computers, which have the potential to leapfrog ordinary computers in areas like materials science, manufacturing optimization and financial services. The prospect of channeling the power of quantum computers to commercial interests has triggered a gold rush as tech giants, such as Google, Intel and IBM, and startups race to develop practical machines.

Progress in the field, however, has been held back by the nature of qubits, which can be built and controlled in different ways. The trouble is all qubits can be easily perturbed, and calculations are derailed when they are. That's why quantum computers typically run at extremely low temperatures in vibration-proof housings.

Quantum computing

Quantum computer makers like their odds for big progress

Google quantum computer leaves old-school supercomputers in the dust

Honeywell fires up the H1, its second-generation quantum computer

Quantum computers could crack today's encrypted messages. That's a problem

Honeywell demonstrated its technique on its 10-qubit H1 quantum computer. Seven of the qubits stored data while the remaining three "ancilla" qubits shepherded the error correction process, which is governed by a conventional computer that steers qubits back on track when a problem is detected.

Achieving quantum error correction

Quantum error correction is a method for detecting and fixing qubit errors so calculations can run longer. Different aspects of QEC, including Honeywell's logical qubits, should enable more advanced algorithms.

Honeywell didn't actually perform any computation during its demonstration, but showed that it could initialize the system, correct qubit errors during operations, and read the results afterward.

Using the smallest possible number of physical qubits to make a logical qubit is an important consideration in improving quantum computers. Today's machines only have a few dozen qubits at best, and many expect quantum computers to need thousands of logical qubits to become really useful. Google said in May it expects to require about 1,000 physical qubits for each logical qubit as it moves to deliver a practical quantum computer by 2029.

Every other quantum computing company is trying to improve qubit operations, too. That work includes not just error correction, but also making qubits less prone to errors in the first place, lengthening the time multiple qubits stay entangled so they can perform calculations, and compensating for errors after calculations are complete. Even Amazon, which offers a quantum computing service called Braket but hasn't announced any quantum computers of its own, is tackling error correction ideas.

New Honeywell quantum computers on the way

Honeywell makes quantum computers, including the H0 and H1, which uses charged atoms of ytterbium as qubits that can be manipulated with laser beams. "The H2 generation is up and running" in prototype form, Uttley said in a June interview, and the H3 is under active development.

Honeywell's quantum computing unit is merging with Cambridge Quantum Computing, whose expertise is in algorithms and other quantum software matters.

The result, once regulatory hurdles are cleared and the deal closes, should be deeper collaboration that dramatically accelerates progress, said Ilyas Kahn, who's CEO of Cambridge Quantum Computing and slated to take over the merged company, in June.

Also on Wednesday, Honeywell and CQC announced a new quantum computing algorithm that solves optimization problems with fewer qubits.

19.Israeli startup aims to be the Mellanox of quantum

by SARA TOTH STUB
https://www.timesofisrael.com/spotlight/israeli-startup-aims-to-be-the-mellanox-of-quantum/

In 2020, Israeli computing company Mellanox hit the headlines when it was bought for $7 billion by US computing giant Nvidia. Mellanox enables the construction of supercomputers by linking many powerful computers together.

Aharon Brodutch, CEO and cofounder of Canadian-Israeli startup Entangled Networks, is hoping that his company can emulate that success by performing a similar task for quantum computers – widely regarded as the ultra-super-computers of tomorrow.

The promise of quantum computing – based on the behavior of subatomic particles – is huge, but so far they have been unable to deliver in any practical sense. In theory, a quantum computer could reduce the time for complex calculations from years to "seconds," according to Google CEO Sundar Pichai. But the large quantum machines that could solve complicated problems, develop new materials and transmit hacker-proof data, are too fragile to build. They require very cold temperatures and an isolated, noiseless environment to function.

"Each component you add starts making noise, interfering with other components," Brodutch says. "It's incredibly hard to grow and grow and keep the noise down. This is what is basically preventing quantum computers from becoming huge in the very near future."

In quantum computing, information is encoded in qubits, the quantum equivalent of the bits in classical computing that have a value of either zero or one. With today's technology, if more than a few dozen qubits are included in the core of a quantum computer, the resulting noise and vibrations prevent the machine from performing any serious computation.

"These computers have insane computational power. But there is a catch: They need millions of qubits to solve these problems, and currently the state of the art systems have less than 100 qubits. How do you take these fancy science toy projects and scale them up to the point that they can solve problems that are basically unimaginable for classical computers?" says Brodutch. "You have to go above being a science toy, and this is the solution we are providing."

Entangled Networks is developing hardware and software to connect together multiple quantum computers in order to maximize their potential. The company is developing interconnects – hardware that connects together many smaller quantum computers – eventually enabling thousands or millions of qubits to work together without creating the noise that would disrupt them if they were all part of the same device.

"It will create the holy grail of the industry," says Eli Nir, general partner and head of investments at the Jerusalem-based equity investment platform OurCrowd, which is backing the company. "The biggest challenge in quantum computing today is the need to scale up. Entangled may be the only viable approach to solving this."

IBM and other leaders in quantum computing expect to be able to create computers with up to 1,000 qubits by 2024, but the millions of qubits needed to maximize the potential of quantum remain out of reach.

"Going beyond a thousand qubits to a million will require a new, bolder vision of integration that hasn't yet been outlined in a scalable way," says Nadav Katz, a physicist specializing in quantum information at Hebrew University of Jerusalem. "There are some very exciting ideas about how to do this, but this is the next scientific leap that needs to happen."

Brodutch says Entangled Networks has the answer.

“A single core solution will simply never scale up to the point where you can have the kind of computer that can solve unimaginable problems,” he says. Entangled’s approach will advance quantum computers “generations in terms of the computational power,” and will likely be available within a few years, long before the development of larger computing cores, he says.

Brodutch and Nir say the comparison to Mellanox, the third-largest tech exit in Israel’s history, is valid.

“The same solution will exist in quantum,” Brodutch says. “But it’s a completely different task in terms of the hardware.”

Based on the principles of quantum mechanics first outlined by Einstein and his peers, quantum computers use particles like photons, electrons and atoms to encode information, offering significant speed and security advantages over classical computers. Instead of encoding information in binary digits, or sets of zeros and ones, known as bits, each quantum bit or quibit can be not only a zero or one, but also suspended coherently anywhere between these two states, vastly increasing computing power and memory by simultaneously processing an exponentially number of possible states.

Quantum-based networks could also offer major security advantages because information would travel in photons of light that may be physically far from one another, yet connected together by a concept called entanglement. If a hacker tried to access these particles, the entanglement would be harmed and the information would become scrambled, allowing for the detection and prevention of eavesdropping.

Although most quantum computers are still confined to labs, the market is growing more than 30 percent each year, and is expected to reach $1.7 billion by 2026, according to MarketsandMarkets. Quantum computing is set to transform many sectors, starting with chemical and pharmaceutical research, and “anything that requires deep chemistry simulations at the atomic level,” Brodutch says.

“If you are trying to develop a new drug, or a new battery, or a new fertilizer, or a new material then what you do today is you go to the lab and you start doing experiments, but that is very expensive and very time-consuming,” he explains. “What you would want to do is to run a simulation on your computer. But a classical computer simply cannot handle this challenge – not even a super computer.”

But a quantum computer could.

“You just run simulations on your quantum computer until you find the solution, the right molecule,” he says.

The US Department of Energy, along with 50 partner organizations, is building a nationwide quantum-based internet with a more secure mechanism for financial transactions and other sensitive data, eliminating the need for encryption. Google Inc., which was the first in the world to demonstrate the advantage of quantum computers over regular computers, has launched a quantum computing division, as have IBM, Intel and Microsoft. Scientists in China have used quantum computers to perform calculations that would be impossible for traditional computers.

“Quantum computing is making steady and remarkable progress,” Katz says. “However, it is important to understand the magnitude of the scientific and engineering challenge involved. It is extraordinarily hard and will require years of continued effort to push this ahead.”

Quantum computing could contribute to the fields of artificial intelligence, cybersecurity, financial modelling, logistics optimization and many others, Katz says.

20.Can China Turn Engineering Prowess into Quantum Domination?

by Matt Swayne
https://thequantumdaily.com/2021/07/20/the-quantum-insider-insights-can-china-turn-engineering-prowess-into-quantum-domination/

In this edition of The Quantum Insider, we take a deeper dive into recent news that Chinese scientists have smashed quantum supremacy with their superconducting qubit device. They previously hit that milestone with a optical circuit device.

The news, which was described in ArXiv, poses almost as many questions as it answers, such as:

- What does this mean for the big picture of quantum technology development?
- Is this a sign that China is “the” quantum leader, rather than “a” quantum leader?
- How is this development related to other quantum technology work recently reported by Chinese scientists and engineers?
- And how does China’s business climate relate to the nation’s scientific climate.

21.Xanadu awarded DARPA grant to develop novel quantum compiler for NISQ-based machines

by Xanadu
https://www.prnewswire.com/news-releases/xanadu-awarded-darpa-grant-to-develop-novel-quantum-compiler-for-nisq-based-machines-301337111.html

Xanadu, a full-stack quantum computing company developing quantum hardware and software solutions, has been awarded a Defense Advanced Research Projects Agency (DARPA) grant. The grant will enable Xanadu to develop a unique general-purpose "circuit-cutting" compiler which can automatically break down a circuit into a multi-circuit hybrid model—leveraging both classical and quantum computing—which will be ideal for near-term quantum computers.

"With PennyLane, these complex hybrid models can be run for the user seamlessly on the quantum hardware or simulators of their choice." said Nathan Killoran, who heads up Xanadu's Quantum Software & Algorithms team. "Using these tools, we plan to run quantum algorithms which would natively require 100+ qubits using quantum hardware and simulators containing only 10-30 qubits.”

Xanadu created one of the world's first open-source software platforms for quantum computers, known as PennyLane. PennyLane allows users to connect quantum computing hardware and software from key hardware vendors, including Xanadu, Amazon Web Services (AWS), IBM, Google, IonQ, Rigetti, and Microsoft.

Xanadu will leverage the expertise of its in-house team of dedicated quantum programmers and scientists, whose work in quantum computing is globally recognized, to carry out the DARPA-funded research project over a twenty-four-month period. "If successful, this project will have a wide impact on the entire community working with present-day quantum computers," said Christian Weedbrook, the company's founder and CEO. "It will allow everyone to run larger-scale quantum computations than they currently can—without needing access to more powerful quantum processors."

This is Xanadu's second grant from DARPA, after successfully completing an initial grant on quantum machine learning using PennyLane.

22.Quantum Matters: The Good, The Bad and The Ugly of Quantum Cybersecurity

by Karina Robinson
https://thequantumdaily.com/2021/07/19/quantum-matters-the-good-the-bad-and-the-ugly-of-quantum-cybersecurity/

Imagine two scenarios.

An assassination in Sarajevo. The subsequent chain of events ultimately leads to a world war. An estimated 20 million people die.

A small US bank succumbs to a cyberattack. Amidst carefully placed misinformation campaigns, bank runs and riots, the repercussions start to drag down the financial system. The US blames Russia, calls on NATO under Article 5, where an attack on one is an attack on all, and step-by-step the world explodes into the Third World War.

What unifies these two scenarios is that we are living in an era reminiscent of pre-World War I: the seeds of conflict are sown, irrigated by mistrust, and one spark can start a wildfire.

Last month at their Geneva summit Joe Biden made clear to Vladimir Putin where the US red lines in cybersecurity lie. "Certain critical infrastructure should be off-limits to attack, period," said the US President. One of the 16 sectors mentioned was financial services. It is a given that the message was also aimed at China, Iran and other hostile states with a track record of cyberattacks.

The US government has been in contact with American banks this year to chivy them into increasing their cyber defences, while Federal Reserve Chairman Jerome Powell stated that cyberattacks are the biggest risk to the system. They can trigger a liquidity run and lead to solvency issues.

One of the most worrying possibilities is a supply chain attack. In a little-publicised paper published by the New York Federal Reserve, Cyber Risk and the US Financial System: A Pre-Mortem Analysis, the authors note that an attack on a significant service provider which connects small and medium sized banks has the potential to cause a

systemic event. The concentration of banks using the few existing cloud providers, like AWS or Microsoft's Azure, for instance, is a clear risk.

The authors also note that in a five-day cyber attack, nearly half of US financial institutions would run out of reserves by day five.

The top concern is not so much a provocation, as a misjudgement, ultimately leading to WWIII. Take the recent Colonial Pipeline attack by DarkSide. They planned to attack the business side, not the operational side, which is responsible for transmitting roughly 45% of East Coast fuel. They knew the latter would be perceived as an attack on infrastructure, bringing the might of the US intelligence services down on them for straying into the political arena.

"We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for our other motives," they swiftly posted on their Dark Web page, as they sought to excuse their error and distance themselves from suspicions of links to the Russian government.

There is no easy solution to the uncertainty of who is behind a cyber attack, nor to mishaps prevalent in a digital world.

But there is a clear need for key sectors to take a big step up in cybersecurity. Not least with China – which just celebrated the 100th anniversary of the Communist Party amid Taiwan fly-overs – on what looks ever more likely to be a collision course with the West.

Paradoxically, the quantum industry may be the answer to cybersecurity, while also being its biggest threat. The creation of quantum keys which are certifiably random – unlike the current RSA encryption and other standard ones – could provide hacker-free security. At least eleven global banks are exploring quantum safe protocols for security, ranging from JP Morgan to BNP Paribas and RBC of Canada, as reported here by The Quantum Daily (TQD). Around thirty-five quantum companies in countries ranging from Poland to Singapore are working on quantum cybersecurity products.

A handful of years down the line powerful quantum computers may be able to decrypt the data already being harvested by ransomware gangs and hostile nation states – yet another reason to experiment with current quantum cryptography.

Although information is hard to come by, China reportedly has quantum key distribution technology over fibre optic cable between Beijing and Shanghai. In essence, a quantum internet, providing hundreds of kilometres of totally secure communications.

The West is intent on catching up, with governments and companies spending large sums. Germany, for instance, announced in May a €2bn investment in quantum and related technologies, while a month later British start-up Arquit announced a link with defence company Northrop Grumman to explore its own end-to-end quantum encryption. Meanwhile, the US Department of Energy last year unveiled a blueprint for a quantum internet.

The Cold War arms race mostly involved creating weapons of destruction, the so-called Mutually Assured Destruction (MAD) doctrine which, arguably, kept the peace over many decades. In the 21st century, the most important advance in keeping world peace will be security and protection: Mutually Assured Defence – not as MAD.

23.Time-varying quantum channel models for superconducting qubits

by Josu Etxezarreta Martinez, Patricio Fuentes, Pedro Crespo & Javier Garcia-Frias
https://www.nature.com/articles/s41534-021-00448-5

The decoherence effects experienced by the qubits of a quantum processor are generally characterized using the amplitude damping time ($T1$) and the dephasing time ($T2$). Quantum channel models that exist at the time of writing assume that these parameters are fixed and invariant. However, recent experimental studies have shown that they exhibit a time-varying (TV) behaviour. These time-dependant fluctuations of $T1$ and $T2$, which become even more pronounced in the case of superconducting qubits, imply that conventional static quantum channel models do not capture the noise dynamics experienced by realistic qubits with sufficient precision. In this article, we study how the fluctuations of $T1$ and $T2$ can be included in quantum channel models. We propose the idea of time-varying quantum channel (TVQC) models, and we show how they provide a more realistic portrayal of decoherence effects than static models in some instances. We also discuss the divergence that exists between TVQCs and their static counterparts by means of a metric known as the diamond norm. In many circumstances this divergence can be significant, which indicates that the time-dependent nature of decoherence must be considered, in order to construct models that capture the real nature of quantum devices.

24.SES-led Consortium to Define Quantum Encryption for Luxembourg

by RAY SHARMA
https://www.thefastmode.com/technology-solutions/20237-ses-led-consortium-to-define-quantum-encryption-for-luxembourg

The Luxembourg's Quantum Communications Infrastructure project (LuxQCI) aims to create a secure communications shield against cyber threats based on quantum technology.

To design the LuxQCI, Luxembourg has put in place a consortium comprising InCert, itrust consulting, LuxConnect, LuxTrust and the University of Luxembourg (SnT), that is led by SES's fully-owned affiliate SES Techcom.

One of the LuxQCI's main functions will be to ensure quantum key distribution (QKD), an ultra-secure form of encryption that uses the principles of quantum mechanics. Enabled via satellites, QKD can secure confidential data, power grids, government communications and digital transactions, including against attacks by quantum computers. Once operational, LuxQCI will guarantee the security of digital transactions and of confidential information transfer over geographically dispersed areas. Early users of the infrastructure will be governmental and institutional authorities and business sectors requiring ultra-secure data transmission. QCI will ultimately evolve into a Quantum Internet, linking quantum processors and sensors and enabling an EU-wide distributed quantum computing and communication capability.

The LuxQCI is an integral part of the European Quantum Communication Infrastructure (EuroQCI), an initiative from the European Commission. The LuxQCI project will include among other key objectives the design of the country's national QCI, integrating both terrestrial and space-based Quantum Key Distribution (QKD) into an innovative hybrid Key Management System (hKMS). It will also plan for the integration of Luxembourg's national QCI with other European QCI initiatives.

25.Private Israeli spyware used to hack cellphones of journalists, activists worldwide

by Dana Priest, Craig Timberg and Souad Mekhennet
https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

Military-grade spyware licensed by an Israeli firm to governments for tracking terrorists and criminals was used in attempted and successful hacks of 37 smartphones belonging to journalists, human rights activists, business executives and two women close to murdered Saudi journalist Jamal Khashoggi, according to an investigation by The Washington Post and 16 media partners.

The phones appeared on a list of more than 50,000 numbers that are concentrated in countries known to engage in surveillance of their citizens and also known to have been clients of the Israeli firm, NSO Group, a worldwide leader in the growing and largely unregulated private spyware industry, the investigation found.

The list does not identify who put the numbers on it, or why, and it is unknown how many of the phones were targeted or surveilled. But forensic analysis of the 37 smartphones shows that many display a tight correlation between time stamps associated with a number on the list and the initiation of surveillance, in some cases as brief as a few seconds.

Forbidden Stories, a Paris-based journalism nonprofit, and Amnesty International, a human rights group, had access to the list and shared it with the news organizations, which did further research and analysis. Amnesty's Security Lab did the forensic analyses on the smartphones.

The numbers on the list are unattributed, but reporters were able to identify more than 1,000 people spanning more than 50 countries through research and interviews on four continents: several Arab royal family members, at least 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials — including cabinet ministers, diplomats, and military and security officers. The numbers of several heads of state and prime ministers also appeared on the list.

Among the journalists whose numbers appear on the list, which dates to 2016, are reporters working overseas for several leading news organizations, including a small number from CNN, the Associated Press, Voice of America, the New York Times, the Wall Street Journal, Bloomberg News, Le Monde in France, the Financial Times in London and Al Jazeera in Qatar.

The targeting of the 37 smartphones would appear to conflict with the stated purpose of NSO's licensing of the Pegasus spyware, which the company says is intended only for use in surveilling terrorists and major criminals. The

evidence extracted from these smartphones, revealed here for the first time, calls into question pledges by the Israeli company to police its clients for human rights abuses.

The media consortium, titled the Pegasus Project, analyzed the list through interviews and forensic analysis of the phones, and by comparing details with previously reported information about NSO. Amnesty's Security Lab examined 67 smartphones where attacks were suspected. Of those, 23 were successfully infected and 14 showed signs of attempted penetration.

For the remaining 30, the tests were inconclusive, in several cases because the phones had been replaced. Fifteen of the phones were Android devices, none of which showed evidence of successful infection. However, unlike iPhones, Androids do not log the kinds of information required for Amnesty's detective work. Three Android phones showed signs of targeting, such as Pegasus-linked SMS messages.

Amnesty shared backup copies of data on four iPhones with Citizen Lab, which confirmed that they showed signs of Pegasus infection. Citizen Lab, a research group at the University of Toronto that specializes in studying Pegasus, also conducted a peer review of Amnesty's forensic methods and found them to be sound.

In lengthy responses before publication, NSO called the investigation's findings exaggerated and baseless. It also said it does not operate the spyware licensed to its clients and "has no insight" into their specific intelligence activities.

After publication, NSO chief executive Shalev Hulio expressed concern in a phone interview with The Post about some of the details he had read in Pegasus Project stories Sunday, while continuing to dispute that the list of more than 50,000 phone numbers had anything to do with NSO or Pegasus.

"The company cares about journalists and activists and civil society in general," Hulio said. "We understand that in some circumstances our customers might misuse the system and, in some cases like we reported in [NSO's] Transparency and Responsibility Report, we have shut down systems for customers who have misused the system."

He said that in the past 12 months NSO had terminated two contracts over allegations of human rights abuses, but he declined to name the countries involved.

"Every allegation about misuse of the system is concerning me," he said. "It violates the trust that we give customers. We are investigating every allegation."

NSO describes its customers as 60 intelligence, military and law enforcement agencies in 40 countries, although it will not confirm the identities of any of them, citing client confidentiality obligations. The consortium found many of the phone numbers in at least 10 country clusters, which were subjected to deeper analysis: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia and the United Arab Emirates. Citizen Lab also has found evidence that all 10 have been clients of NSO, according to Bill Marczak, a senior research fellow.

Forbidden Stories organized the media consortium's investigation, and Amnesty provided analysis and technical support but had no editorial input. Amnesty has openly criticized NSO's spyware business and supported an unsuccessful lawsuit against the company in an Israeli court seeking to have its export license revoked. After the investigation began, several reporters in the consortium learned that they or their family members had been successfully attacked with Pegasus spyware.

- More than 50,000 smartphone numbers appear on a list of phones concentrated in countries known to engage in surveillance on their citizens and also known to have been clients of NSO Group, an Israeli firm

that is a worldwide leader in cybersurveillance. The numbers span more than 50 countries around the globe.

- The greatest number was in Mexico, where more than 15,000 numbers, including those belonging to politicians, union representatives, journalists and other government critics, were on the list.
- A large share of numbers were in the Middle East, including in Qatar, the UAE, Bahrain and Yemen. The UAE, Saudi Arabia and Bahrain are reported to be among NSO clients.
- In India, the numbers of phones belonging to hundreds of journalists, activists, opposition politicians, government officials and business executives were on the list, as were numbers in several other countries in the region, including Azerbaijan, Kazakhstan and Pakistan.
- More than 1,000 French numbers were on the list. In Hungary, numbers associated with at least two media magnates were among hundreds on the list, and the phones of two working journalists were targeted and infected, forensic analysis showed.

Beyond the personal intrusions made possible by smartphone surveillance, the widespread use of spyware has emerged as a leading threat to democracies worldwide, critics say. Journalists under surveillance cannot safely gather sensitive news without endangering themselves and their sources. Opposition politicians cannot plot their campaign strategies without those in power anticipating their moves. Human rights workers cannot work with vulnerable people — some of whom are victims of their own governments — without exposing them to renewed abuse.

For example, Amnesty's forensics found evidence that Pegasus was targeted at the two women closest to Saudi columnist Khashoggi, who wrote for The Post's Opinions section. The phone of his fiancee, Hatice Cengiz, was successfully infected during the days after his murder in Turkey on Oct. 2, 2018, according to a forensic analysis by Amnesty's Security Lab. Also on the list were the numbers of two Turkish officials involved in investigating his dismemberment by a Saudi hit team. Khashoggi also had a wife, Hanan Elatr, whose phone was targeted by someone using Pegasus in the months before his killing. Amnesty was unable to determine whether the hack was successful.

"This is nasty software — like eloquently nasty," said Timothy Summers, a former cybersecurity engineer at a U.S. intelligence agency and now director of IT at Arizona State University. With it "one could spy on almost the entire world population. … There's not anything wrong with building technologies that allows you to collect data; it's necessary sometimes. But humanity is not in a place where we can have that much power just accessible to anybody."

In response to detailed questions from the consortium before publication, NSO said in a statement that it did not operate the spyware it licensed to clients and did not have regular access to the data they gather. The company also said its technologies have helped prevent attacks and bombings and broken up rings that trafficked in drugs, sex and children. "Simply put, NSO Group is on a life-saving mission, and the company will faithfully execute this mission undeterred, despite any and all continued attempts to discredit it on false grounds," NSO said. "Your sources have supplied you with information that has no factual basis, as evidenced by the lack of supporting documentation for many of the claims."

The company denied that its technology was used against Khashoggi, or his relatives or associates.

"As NSO has previously stated, our technology was not associated in any way with the heinous murder of Jamal Khashoggi. This includes listening, monitoring, tracking, or collecting information. We previously investigated this claim, immediately after the heinous murder, which again, is being made without validation."

Thomas Clare, a libel attorney hired by NSO, said that the consortium had "apparently misinterpreted and mischaracterized crucial source data on which it relied" and that its reporting contained flawed assumptions and factual errors.

"NSO Group has good reason to believe that this list of 'thousands of phone numbers' is not a list of numbers targeted by governments using Pegasus, but instead, may be part of a larger list of numbers that might have been used by NSO Group customers for other purposes," Clare wrote.

In response to follow-up questions, NSO called the 50,000 number "exaggerated" and said it was far too large to represent numbers targeted by its clients. Based on the questions it was being asked, NSO said, it had reason to believe that the consortium was basing its findings "on misleading interpretation of leaked data from accessible and overt basic information, such as HLR Lookup services, which have no bearing on the list of the customers targets of Pegasus or any other NSO products … we still do not see any correlation of these lists to anything related to use of NSO Group technologies."

The term HLR, or Home Location Register, refers to a database that is essential to operating cellular phone networks. Such registers keep records on the networks of cellphone users and their general locations, along with other identifying information that is used routinely in routing calls and texts. HLR lookup services operate on the SS7 system that cellular carriers use to communicate with each other. The services can be used as a step toward spying on targets.

Telecommunications security expert Karsten Nohl, chief scientist for Security Research Labs in Berlin, said that he does not have direct knowledge of NSO's systems but that HLR lookups and other SS7 queries are widely and inexpensively used by the surveillance industry — often for just tens of thousands of dollars a year.

"It's not difficult to get that access. Given the resources of NSO, it'd be crazy to assume that they don't have SS7 access from at least a dozen countries," Nohl said. "From a dozen countries, you can spy on the rest of the world."

Pegasus was engineered a decade ago by Israeli ex-cyberspies with government-honed skills. The Israeli Defense Ministry must approve any license to a government that wants to buy it, according to previous NSO statements.

"As a matter of policy, the State of Israel approves the export of cyber products exclusively to governmental entities, for lawful use, and only for the purpose of preventing and investigating crime and counterterrorism, under end-use/end user certificates provided by the acquiring government," a spokesperson for the Israeli defense establishment said Sunday. "In cases where exported items are used in violation of export licenses or end-use certificates, appropriate measures are taken."

The numbers of about a dozen Americans working overseas were discovered on the list, in all but one case while using phones registered to foreign cellular networks. The consortium could not perform forensic analysis on most of these phones. NSO has said for years that its product cannot be used to surveil American phones. The consortium did not find evidence of successful spyware penetration on phones with the U.S. country code.

"We also stand by our previous statements that our products, sold to vetted foreign governments, cannot be used to conduct cybersurveillance within the United States, and no customer has ever been granted technology that would enable them to access phones with U.S. numbers," the company said in its statement. "It is technologically impossible and reaffirms the fact your sources' claims have no merit."

Apple and other smartphone manufacturers are years into a cat-and-mouse game with NSO and other spyware makers.

"Apple unequivocally condemns cyberattacks against journalists, human rights activists and others seeking to make the world a better place," said Ivan Krstić, head of Apple Security Engineering and Architecture. "For over a decade, Apple has led the industry in security innovation and, as a result, security researchers agree iPhone is the safest, most secure consumer mobile device on the market. Attacks like the ones described are highly sophisticated, cost millions of dollars to develop, often have a short shelf life and are used to target specific individuals. While that means they are not a threat to the overwhelming majority of our users, we continue to work tirelessly to defend all our customers, and we are constantly adding new protections for their devices and data."

Some Pegasus intrusion techniques detailed in a 2016 report were changed in a matter of hours after they were made public, underscoring NSO's ability to adapt to countermeasures.

Pegasus is engineered to evade defenses on iPhones and Android devices and to leave few traces of its attack. Familiar privacy measures like strong passwords and encryption offer little help against Pegasus, which can attack phones without any warning to users. It can read anything on a device that a user can, while also stealing photos, recordings, location records, communications, passwords, call logs and social media posts. Spyware also can activate cameras and microphones for real-time surveillance.

"There is just nothing from an encryption standpoint to protect against this," said Claudio Guarnieri, a.k.a. "Nex," the Amnesty Security Lab's 33-year-old Italian researcher who developed and performed the digital forensics on 37 smartphones that showed evidence of Pegasus attacks.

That sense of helplessness makes Guarnieri, who often dresses head-to-toe in black, feel as useless as a 14th-century doctor confronting the Black Plague without any useful medication. "Primarily I'm here just to keep the death count," he said.

The attack can begin in different ways. It can come from a malicious link in an SMS text message or an iMessage. In some cases, a user must click on the link to start the infection. In recent years, spyware companies have developed what they call "zero-click" attacks, which deliver spyware simply by sending a message to a user's phone that produces no notification. Users do not even need to touch their phones for infections to begin.

Many countries have laws pertaining to traditional wiretapping and interception of communications, but few have effective safeguards against deeper intrusions made possible by hacking into smartphones. "This is more devious in a sense because it really is no longer about intercepting communications and overhearing conversation. … This covers all of them and goes way beyond that," Guarnieri said. "It has raised a lot of questions from not only human rights, but even national constitutional laws as to is this even legal?"

Clare, NSO's attorney, attacked the forensic examinations as "a compilation of speculative and baseless assumptions" built on assumptions based on earlier reports. He also said, "NSO does not have insight into the specific intelligence activities of its customers."

The Pegasus Project's findings are similar to previous discoveries by Amnesty, Citizen Lab and news organizations worldwide, but the new reporting offers a detailed view of the personal consequences and scale of surveillance and its abuses.

The consortium analyzed the list and found clusters of numbers with similar country codes and geographical focus that align with previous reporting and additional research about NSO clients overseas. For example, Mexico has been previously identified in published reports and documents as an NSO client, and entries on the list are clustered by Mexican country code, area code and geography. In several cases, clusters also contained numbers from other countries.

In response to questions from reporters, spokespeople for the countries with clusters either denied Pegasus was used or denied that their country had abused their powers of surveillance.

Hungarian Prime Minister Viktor Orban's office said any surveillance carried out by that nation is done in accordance with the law.

"In Hungary, state bodies authorized to use covert instruments are regularly monitored by governmental and non-governmental institutions," the office said. "Have you asked the same questions of the governments of the United States of America, the United Kingdom, Germany or France?"

Moroccan authorities responded: "It should be recalled that the unfounded allegations previously published by Amnesty International and conveyed by Forbidden Stories have already been the subject of an official response from the Moroccan authorities, who have categorically rejected these allegations."

Vincent Biruta, Rwanda's foreign affairs minister, also denied the use of Pegasus.

"Rwanda does not use this software system, as previously confirmed in November 2019, and does not possess this technical capability in any form," Biruta said. "These false accusations are part of an ongoing campaign to cause tensions between Rwanda and other countries, and to sow disinformation about Rwanda domestically and internationally."

.
.
.

Snowden's legacy

Today's thriving international spyware industry dates back decades but got a boost after the unprecedented 2013 disclosure of highly classified National Security Agency documents by contractor Edward Snowden. They revealed that the NSA could obtain the electronic communications of almost anyone because it had secret access to the transnational cables carrying Internet traffic worldwide and data from Internet companies such as Google and giant telecommunications companies such as AT&T.

Even U.S. allies in Europe were shocked by the comprehensive scale of the American digital spying, and many national intelligence agencies set out to improve their own surveillance abilities. For-profit firms staffed with midcareer retirees from intelligence agencies saw a lucrative market-in-waiting free from the government regulations and oversight imposed on other industries.

The dramatic expansion of end-to-end encryption by Google, Microsoft, Facebook, Apple and other major technology firms also prompted law enforcement and intelligence officials to complain they had lost access to the communications of legitimate criminal targets. That in turn sparked more investment in technologies, such as Pegasus, that worked by targeting individual devices.

.
.
.

26.European Commission's Horizon Europe and Canada's NSERC Team to Issue a Call for Proposals with an €8 Million Budget

https://quantumcomputingreport.com/european-commissions-horizon-europe-and-canadas-nserc-team-to-issue-a-call-for-proposals-with-an-e8-million-11-9m-cad-9-4m-usd-budget/

The European Commission's Horizon Europe and Canada's Natural Sciences and Engineering Research Council of Canada (NSERC) are partnering to issue a call for joint EU-CAN proposals for research on quantum technologies. Each one will provide funding of up to €4 Million (about $6M CAD or $4.7M USD) for projects related to quantum communication, quantum computing, quantum simulation or quantum sensing. The expected award to each selected EU-Canada consortium is about €1.33 Million (about $2M CAD or $1.57M USD) for projects expect to range from 36 to 60 months in duration. The EC will pay their funds to the European participants and the NSERC will pay their funds to the Canadian participants. Additional information about this joint call for proposals is available in a brief news release and also a program description available on the NSERC website.

27.Unconventional superconductor acts the part of a promising quantum computing platform

by Dina Genkina
https://phys.org/news/2021-07-unconventional-superconductor-quantum-platform.html

Scientists on the hunt for an unconventional kind of superconductor have produced the most compelling evidence to date that they've found one. In a pair of papers, researchers at the University of Maryland's (UMD) Quantum Materials Center (QMC) and colleagues have shown that uranium ditelluride (or UTe_2 for short) displays many of the hallmarks of a topological superconductor—a material that may unlock new ways to build quantum computers and other futuristic devices.

"Nature can be wicked," says Johnpierre Paglione, a professor of physics at UMD, the director of QMC and senior author on one of the papers. "There could be other reasons we're seeing all this wacky stuff, but honestly, in my career, I've never seen anything like it."

All superconductors carry electrical currents without any resistance. It's kind of their thing. The wiring behind your walls can't rival this feat, which is one of many reasons that large coils of superconducting wires and not normal copper wires have been used in MRI machines and other scientific equipment for decades.

But superconductors achieve their super-conductance in different ways. Since the early 2000s, scientists have been looking for a special kind of superconductor, one that relies on an intricate choreography of the subatomic particles that actually carry its current.

This choreography has a surprising director: a branch of mathematics called topology. Topology is a way of grouping together shapes that can be gently transformed into one another through pushing and pulling. For example, a ball of dough can be shaped into a loaf of bread or a pizza pie, but you can't make it into a donut without poking a hole in it. The upshot is that, topologically speaking, a loaf and a pie are identical, while a donut is different. In a topological superconductor, electrons perform a dance around each other while circling something akin to the hole in the center of a donut.

Unfortunately, there's no good way to slice a superconductor open and zoom in on these electronic dance moves. At the moment, the best way to tell whether or not electrons are boogieing on an abstract donut is to observe how a material behaves in experiments. Until now, no superconductor has been conclusively shown to be topological, but the new papers show that UTe_2 looks, swims and quacks like the right kind of topological duck.

One study, by Paglione's team in collaboration with the group of Aharon Kapitulnik at Stanford University, reveals that not one but two kinds of superconductivity exist simultaneously in UTe_2. Using this result, as well as the way light is altered when it bounces off the material (in addition to previously published experimental evidence), they were able to narrow down the types of superconductivity that are present to two options, both of which theorists believe are topological. They published their findings on July 15, 2021, in the journal *Science*.

In another study, a team led by Steven Anlage, a professor of physics at UMD and a member of QMC, revealed unusual behavior on the surface of the same material. Their findings are consistent with the long-sought-after phenomenon of topologically protected Majorana modes. Majorana modes, exotic particles that behave a bit like half of an electron, are predicted to arise on the surface of topological superconductors. These particles particularly excite scientists because they might be a foundation for robust quantum computers. Anlage and his team reported their results in a paper published May 21, 2021 in the journal *Nature Communications*.

Superconductors only reveal their special characteristics below a certain temperature, much like water only freezes below zero Celsius. In normal superconductors, electrons pair up into a two-person conga line, following each other through the metal. But in some rare cases, the electron couples perform a circular dance around each other, more akin to a waltz. The topological case is even more special—the circular dance of the electrons contains a vortex, like the eye amidst the swirling winds of a hurricane. Once electrons pair up in this way, the vortex is hard to get rid of, which is what makes a topological superconductor distinct from one with a simple, fair-weather electron dance.

Back in 2018, Paglione's team, in collaboration with the team of Nicholas Butch, an adjunct associate professor of physics at UMD and a physicist at the National Institute of Standards and Technology (NIST), unexpectedly discovered that UTe_2 was a superconductor. Right away, it was clear that it wasn't your average superconductor. Most notably, it seemed unphased by large magnetic fields, which normally destroy superconductivity by splitting up the electron dance couples. This was the first clue that the electron pairs in UTe_2 hold onto each other more tightly than usual, likely because their paired dance is circular. This garnered a lot of interest and further research from others in the field.

"It's kind of like a perfect storm superconductor," says Anlage. "It's combining a lot of different things that no one's ever seen combined before."

In the new *Science* paper, Paglione and his collaborators reported two new measurements that reveal the internal structure of UTe_2. The UMD team measured the material's specific heat, which characterizes how much energy it takes to heat it up by one degree. They measured the specific heat at different starting temperatures and watched it change as the sample became superconducting.

"Normally there's a big jump in specific heat at the superconducting transition," says Paglione. "But we see that there's actually two jumps. So that's evidence of actually two superconducting transitions, not just one. And that's highly unusual."

The two jumps suggested that electrons in UTe_2 can pair up to perform either of two distinct dance patterns.

In a second measurement, the Stanford team shone laser light onto a piece of UTe_2 and noticed that the light reflecting back was a bit twisted. If they sent in light bobbing up and down, the reflected light bobbed mostly up and down but also a bit left and right. This meant something inside the superconductor was twisting up the light and not untwisting it on its way out.

Kapitulnik's team at Stanford also found that a magnetic field could coerce UTe_2 into twisting light one way or the other. If they applied a magnetic field pointing up as the sample became superconducting, the light coming out would be tilted to the left. If they pointed the magnetic field down, the light tilted to the right. This told that researchers that, for the electrons dancing inside the sample, there was something special about the up and down directions of the crystal.

To sort out what all this meant for the electrons dancing in the superconductor, the researchers enlisted the help of Daniel F. Agterberg, a theorist and professor of physics at the University of Wisconsin-Milwaukee and a co-author of the *Science* paper. According to the theory, the way uranium and tellurium atoms are arranged inside the UTe_2 crystal allows electron couples to team up in eight different dance configurations. Since the specific heat measurement shows that two dances are going on at the same time, Agterberg enumerated all the different ways to pair these eight dances together. The twisted nature of the reflected light and the coercive power of a magnetic field along the up-down axis cut the possibilities down to four. Previous results showing the robustness of UTe_2's superconductivity under large magnetic fields further constrained it to only two of those dance pairs, both of which form a vortex and indicate a stormy, topological dance.

"What's interesting is that given the constraints of what we've seen experimentally, our best theory points to a certainty that the superconducting state is topological," says Paglione.

If the nature of superconductivity in a material is topological, the resistance will still go to zero in the bulk of the material, but on the surface something unique will happen: Particles, known as Majorana modes, will appear and form a fluid that is not a superconductor. These particles also remain on the surface despite defects in the material or small disruptions from the environment. Researchers have proposed that, thanks to the unique properties of these particles, they might be a good foundation for quantum computers. Encoding a piece of quantum information into several Majoranas that are far apart makes the information virtually immune to local disturbances that, so far, have been the bane of quantum computers.

Anlage's team wanted to probe the surface of UTe_2 more directly to see if they could spot signatures of this Majorana sea. To do that, they sent microwaves towards a chunk UTe_2, and measured the microwaves that came out on

the other side. They compared the output with and without the sample, which allowed them to test properties of the bulk and the surface simultaneously.

The surface leaves an imprint on the strength of the microwaves, leading to an output that bobs up and down in sync with the input, but slightly subdued. But since the bulk is a superconductor, it offers no resistance to the microwaves and doesn't change their strength. Instead, it slows them down, causing delays that make the output bob up and down out of sync with the input. By looking at the out-of-sync parts of the response, the researchers determined how many of the electrons inside the material participate in the paired dance at various temperatures. They found that the behavior agreed with the circular dances suggested by Paglione's team.

Perhaps more importantly, the in-sync part of the microwave response showed that the surface of UTe_2 isn't superconducting. This is unusual, since superconductivity is usually contagious: Putting a regular metal close to a superconductor spreads superconductivity to the metal. But the surface of UTe_2 didn't seem to catch superconductivity from the bulk—just as expected for a topological superconductor—and instead responded to the microwaves in a way that hasn't been seen before.

"The surface behaves differently from any superconductor we've ever looked at," Anlage says. "And then the question is 'What's the interpretation of that anomalous result?' And one of the interpretations, which would be consistent with all the other data, is that we have this topologically protected surface state that is kind of like a wrapper around the superconductor that you can't get rid of."

It might be tempting to conclude that the surface of UTe_2 is covered with a sea of Majorana modes and declare victory. However, extraordinary claims require extraordinary evidence. Anlage and his group have tried to come up with every possible alternative explanation for what they were observing and systematically ruled them out, from oxidization on the surface to light hitting the edges of the sample. Still, it is possible a surprising alternative explanation is yet to be discovered.

"In the back of your head you're always thinking 'Oh, maybe it was cosmic rays', or 'Maybe it was something else,'" says Anlage. "You can never 100% eliminate every other possibility."

For Paglione's part, he says the smoking gun will be nothing short of using surface Majorana modes to perform a quantum computation. However, even if the surface of UTe_2 truly has a bunch of Majorana modes, there's currently no straightforward way to isolate and manipulate them. Doing so might be more practical with a thin film of UTe_2 instead of the (easier to produce) crystals that were used in these recent experiments.

"We have some proposals to try to make thin films," Paglione says. "Because it's uranium and it's radioactive, it requires some new equipment. The next task would be to actually try to see if we can grow films. And then the next task would be to try to make devices. So that would require several years, but it's not crazy."

Whether UTe_2 proves to be the long-awaited topological superconductor or just a pigeon that learned to swim and quack like a duck, both Paglione and Anlage are excited to keep finding out what the material has in store.

"It's pretty clear though that there's a lot of cool physics in the material," Anlage says. "Whether or not it's Majoranas on the surface is certainly a consequential issue, but it's exploring novel physics which is the most exciting stuff."

28.Quantware Launches the World's First Commercially Available Superconducting Quantum Processors, Accelerating the Advent of the Quantum Computer.

by QuantWare
https://www.design-reuse.com/news/50309/quantware-superconducting-quantum-processor.html

Today Dutch startup QuantWare has launched the world's first commercially available superconducting processor for quantum computers (QPU). This is the first time superconducting quantum processors have been available 'off the shelf', a development with the potential to significantly accelerate the quantum computing revolution.

Quantum technology promises to significantly expand the amount of data computers are able to process, which could have huge implications for fields such as A.I., medicine, business intelligence, and cybersecurity. But the quantum industry is still young and scaling is difficult. Companies building parts for quantum computers need qubits, the microscopic objects that make quantum computing possible, but it is often cost prohibitive for them to produce them themselves. QuantWare's superconducting QPUs eliminate that barrier and may be instrumental in accelerating the development of the quantum computer market.

Superconducting is the leading and most mature approach to quantum processors - Google achieved "quantum supremacy" in 2019 using superconducting QPUs. While other QPUs are already available "off the shelf", this is the first time a *superconducting* QPU has been easily available in productised form, leveling the playing field for quantum experimentation.

QuantWare's proprietary product, Soprano, is a 5-qubit QPU. In an article published by **Ars Technica**, QuantWare shared that "the fidelities of each qubit will be 99.9 percent, which should keep the error rate manageable." 5 qubits is sufficient for the immediate customer base QuantWare expects to attract, namely research institutions and university labs.

- "Our Soprano QPU is what the Intel 4004 was for the semiconductor business," says QuantWare co-founder Matthijs Rijlaarsdam. "Superconducting qubits are highly customizable, easy to control and very scalable. That practicality makes superconducting QPUs by far the most likely candidate for near-term quantum computing applications."

- QuantWare's products significantly lower the costs traditionally required to create quantum technology. The company has already demonstrated its approach by supplying a QPU to the ImpaQT project, the world's first multi-company quantum computer.

- The world has been promised quantum computers for a long time - computers that can solve problems previously unsolvable by traditional computers, finishing calculations within days or minutes instead of thousands of years. However, large quantum computers are needed in order to have a chance to prove this claim in a challenge known as achieving "quantum supremacy" or "quantum advantage". However, large quan-

tum processors are only available to large companies like IBM and Google to dominate the field. QuantWare aims to make such processors a possibility for all companies and researchers in the space.

"The race towards useful Quantum Computation is heating up, but still reserved to a small group of companies. By making QPUs more available, we will speed up the development of practical quantum-driven solutions to the world's biggest problems." said QuantWare co-founder Dr. Alessandro Bruno.

Another way to achieve "Quantum Advantage" is by designing a chip specifically for a particular application. The startup wants to exploit this by making co-designed QPUs together with software companies to allow them to develop processors specialized in their algorithms.

QuantWare was founded in 2020 by quantum engineer Dr. Alessandro Bruno and Delft University of Technology (TU Delft) graduate MSc Matthijs Rijlaarsdam. They met while doing research at QuTech, a quantum technology research institute at TU Delft in the Netherlands. The company recently closed their pre-seed funding round, meaning the company has now raised €1.15M. They plan to quickly expand their team and upgrade their processors towards higher qubit numbers. One of their growth goals for the rest of the year is to expand fabrication capabilities and partnerships - QuantWare hopes to become a collaborative bridge between quantum companies worldwide. The company is already looking for new operational facilities, as they expect to outgrow their current building within months. QuantWare's first two products, Crescendo and Soprano, are now available for pre-order.

29.Taking Quantum Cryptography Out of the Spotlight

by Edwin Cartlidge
https://www.osa-opn.org/home/newsroom/2021/july/taking_quantum_cryptography_out_of_the_spotlight/

In theory, quantum cryptography enables two or more people to communicate with one another in complete secrecy. In practice, eavesdroppers can exploit weaknesses in the equipment used to send and receive secret keys.

Researchers in Singapore have now shown how practice can be brought closer to theory—by inserting a fairly simple passive device to prevent eavesdropping attacks involving bright light (Phys. Rev. X, doi: 10.1103/PRXQuantum.2.030304). They reckon their solution could be widely adopted in future, having shown that it can be applied to a number of popular cryptographic schemes.

QKD's bright-light vulnerability

The power of quantum key distribution (QKD) stems from the fact that the secret keys used to encrypt and decrypt messages are encoded using the quantum properties of photons or other particles. This means that any eavesdropper—known conventionally as Eve—who's trying to intercept the key on its way from the sender (Alice) to receiver (Bob) will reveal themselves through their act of quantum measurement.

However, QKD has an Achilles' heel: its reliance on very weak pulses of light to encode data at the single-photon level. By exposing either the sending or receiving equipment to bright light, Eve can transform these devices into classical instruments—and therefore remove the quantum-enabled secrecy.

Power-limiting solution

In their recent work, Charles Lim, Gong Zhang and colleagues at the National University of Singapore have developed a system to limit the optical power that such attacks rely on. Their device exploits an acrylic prism with a negative thermo-optical coefficient. Incoming light generates a gradient in temperature, and therefore in refractive-index, inside the prism that turns the acrylic into a concave lens. A small aperture placed behind the prism blocks most of the resulting diverged light beam, diminishing the beam power.

The researchers tested their idea by building the device using prisms with a variety of lengths and with a diaphragm that allowed them to vary the aperture. They found that in all cases the set-up introduced an upper limit on the output power, but that, as expected, longer prisms and smaller apertures yielded the lowest limits, with a roughly 10-cm-long prism and 25-μm-diameter aperture reducing the maximum power to about 1 μW.

The researchers found that the device works well even when dealing with signals of varying wavelength or pulse width, for example. They also showed that it preserved the quality of the signals, having very little impact on photons' intensity, phase or polarization. They acknowledge that there is a trade-off between the (desired) reduction in optical power and (undesired) loss due to the device coupling, but say that this balance can be tailored for different applications.

Application to QKD schemes

Indeed, Lim and colleagues describe in some detail how the device could be employed in specific applications. One of these is centered on "measurement-device-independent QKD", which involves both Alice and Bob generating key bits and sending them to a third (untrusted) party, Charlie. With Charlie merely registering whether or not the bits in each case match one another, rather than measuring their absolute values, Alice and Bob can generate a secret key without having to rely either on the integrity of the detector or on Charlie's honesty.

The weakness of this approach is that Eve can still target the transmitters of Alice and Bob, and thereby carry out a "Trojan-horse attack" by bouncing bright light off either of the devices and using the reflections to gain information on the key bits. The answer, say the Singapore researchers, would be to insert a power limiter between each transmitter and Charlie's detection equipment, thus reducing the rate at which Eve can siphon off photons, such that she no longer gains useful information.

Another application analyzed in the new work involves a more straightforward direct line of communication between Alice and Bob. In this case, Eve could potentially steal a key by using bright light to either damage or "blind" Bob's receiver. The solution in this case would be to insert power limiters at the output of Alice's transmitter and the input of Bob's receiver.

Lim and colleagues reckon that their new device can ensure protection for a broad range of QKD protocols without having to modify pre-existing cryptographic equipment. Claiming that it would also be "compact, robust and cost-effective," they argue that the power limiter has the potential to "become a standard tool for quantum cryptography applications."

30.Google demonstrates vital step towards large-scale quantum computers

by Matthew Sparkes
https://www.newscientist.com/article/2283945-google-demonstrates-vital-step-towards-large-scale-quantum-computers/

Google has shown that its Sycamore quantum computer can detect and fix computational errors, an essential step for large-scale quantum computing, but its current system generates more errors than it solves.

Error-correction is a standard feature for ordinary, or classical, computers, which store data using bits with two possible states: 0 and 1. Transmitting data with extra "parity bits" that warn if a 0 has flipped to 1, or vice versa, means such errors can be found and fixed.

In quantum computing the problem is far more complex as each quantum bit, or qubit, exists in a mixed state of 0 and 1, and any attempt to measure them directly destroys the data. One longstanding theoretical solution to this has been to cluster many physical qubits into a single "logical qubit". Although such logical qubits have been created previously, they hadn't been used for error correction until now.

Julian Kelly at Google AI Quantum and his colleagues have demonstrated the concept on Google's Sycamore quantum computer, with logical qubits ranging in size from five to 21 physical qubits, and found that logical qubit error rates dropped exponentially for each additional physical qubit. The team was able to make careful measurements of the extra qubits that didn't collapse their state but, when taken collectively, still gave enough information to deduce whether errors had occurred.

Kelly says that this means it is possible to create practical, reliable quantum computers in the future. "This is basically our first half step along the path to demonstrate that," he says. "A viable way of getting to really large-scale, error-tolerant computers. It's sort of a look ahead for the devices that we want to make in the future."

The team has managed to demonstrate this solution conceptually but a vast engineering challenge remains. Adding more qubits to each logical qubit brings its own problems as each physical qubit is itself susceptible to errors. The chance of a logical qubit encountering an error rises as the number of qubits inside it increases.

There is a breakeven point in this process, known as the threshold, where the error correction features catch more problems than the increase in qubits bring. Crucially, Google's error correction doesn't yet meet the threshold. To do so will require less noisy physical qubits that encounter fewer errors and larger numbers of them devoted to each logical qubit. The team believes that mature quantum computers will need 1000 qubits to make each logical qubit – Sycamore currently has just 54 physical qubits.

Peter Knight at Imperial College London says Google's research is progress towards something essential for future quantum computers. "If we couldn't do this we're not going to have a large scale machine," he says. "I applaud the fact they've done it, simply because without this, without this advance, you will still have uncertainty about whether the roadmap towards fault tolerance was feasible. They removed those doubts."

But he says it will be a vast engineering challenge to actually meet the threshold and build effective error correction, which would mean building a processor with many more qubits than has been demonstrated until now.

31.Encryption issues account for minority of flaws in encryption libraries – research

by John Leyden
https://portswigger.net/daily-swig/encryption-issues-account-for-minority-of-flaws-in-encryption-libraries-research

An analysis of cryptographic libraries and the vulnerabilities affecting them has concluded that memory handling issues give rise to more vulnerabilities than encryption implementation errors.

The study by academics at Massachusetts Institute of Technology (MIT) involved an examination of eight widely used cryptographic libraries using a combination of sources, including data from the National Vulnerability Database, individual project repositories, and mailing lists, among other sources.

Vulnerabilities in any of these widely used crypto libraries puts portions of web traffic and e-commerce transactions in danger, but the study concluded that coding rigour in the development of encryption technologies compares poorly with comparably complex mainstream software.

For example, a flaw in the widely used OpenSSL library in 2014 gave rise to the infamous Heartbleed vulnerability.

Roll the dice

The study, entitled 'You Really Shouldn't Roll Your Own Crypto: An Empirical Study of Vulnerabilities in Cryptographic Libraries', by researchers Jenny Blessing, Michael Specter, and Daniel Weitzner, found "evidence of a strong correlation between the complexity of these libraries and their (in)security, empirically demonstrating the potential risks of bloated cryptographic codebases."

Only 27.2% of vulnerabilities in cryptographic libraries are cryptographic issues compared to 37.2% of vulnerabilities that are rooted in memory safety issues.

Non-cryptographic source code generally has a lower density of CVEs introduced compared to cryptographic libraries, the researchers found.

"Our findings suggest that cryptographic source code is indeed more brittle and prone to producing security bugs than a comparable amount of source code in a web browser or operating system," the researchers conclude.

"The empirical data leads us to conclude that complexity is an even worse enemy of security in cryptographic software than in non-cryptographic software."

Speaking the same language

The researchers call for a systems-based approach to cryptographic software, as well as emphasizing the dangers of "rolling your own crypto" – meaning that software developers should rely on established libraries and tools instead of developing their own.

The paper provoked a debate on the merits of different coding languages for cryptographic libraires on Twitter, in which a move away from C and C++ towards memory safe programming languages such **Rust** was advocated.

Open source isn't really the answer because even in open source code, such as OpenSSL, errors like Heartbleed can go undetected for years.

Professor Alan Woodward, a computer scientist at the University of Surrey, told *The Daily Swig*: "Languages such as C/C++ are complex to write in and even though modern compilers and tool sets provide some safeguards against memory issues, they continue."

"As an empirical study it's quite useful as a means of showing anyone that wishes to roll their own that they should get a real expert in both cryptography and the languages they are using to check to ensure they haven't made a choice or used a construction that will render the cryptography insecure."

32.BMW Group, AWS Launch 'Quantum Computing Challenge' to Crowd-Source Innovation

by Matt Swayne
https://thequantumdaily.com/2021/07/13/bmw-group-aws-launch-quantum-computing-challenge-to-crowd-source-innovation/

Researchers, start-ups and pioneering companies from the global quantum computing community can propose solutions for specific industrial challenges to the BMW Group Quantum Computing Challenge. Run in collaboration with Amazon Web Services, Inc. (AWS), the Challenge encourages entrants to come up with innovative quantum algorithms and test their solutions on real quantum computing technologies. Quantum computing holds potential to address challenging problems in the automotive sector in complex optimisation, materials research, and – in the form of quantum machine learning – automated driving in tomorrow's world.

Peter Lehnert, Vice President BMW Group Research, New Technologies said, "The technological landscape in the field of quantum computing is only just starting to take shape. Different firms and research institutes are pursuing a variety of approaches. By launching our crowd innovation initiative, we are hoping to tap into additional innovative power that would be beyond the reach of a standard tendering process."

Specific challenges for quantum computing

Experts from the BMW Group have **identified over 50 challenges** at various stages of the value chain where quantum computing could provide a potential benefit in the future. This requires innovative algorithms and a significant improvement of the hardware. The BMW Group has decided to engage the global quantum computing community to help find the best solutions for the immediate future and beyond. The Quantum Computing Challenge will focus on four specific challenges where quantum computing could deliver an advantage over classical computing methods:

- **Optimisation of sensor positions for automated driving functions**
- **Simulation of material deformation in the production process**

- **Optimisation of pre-production vehicle configuration**
- **Machine Learning for automated quality assessment**

The deadline for submissions is 24 September 2021, after which they will be examined and judged by a panel of experts. A final event will take place in December 2021, where the top entrants will have the opportunity to pitch their solutions to the panel of expert judges. The winners will gain the BMW Group as a client and will also be involved in the implementation of the respective pilot projects.

AWS is supporting the BMW Group via the Amazon Quantum Solutions Lab, an expert group of professionals that helped outline the challenge use cases and who will be on the panel that selects the winners. AWS will provide credits for entrants to use Amazon Braket to encourage development and testing of the quantum algorithms submitted. Amazon Braket provides a development environment for users to explore and build quantum algorithms, test them on quantum circuit simulators, and run them on a variety of quantum hardware technologies.

"Quantum computing is in its early stages but its long-term impact promises to be transformational for many industries," said Bill Vass, Vice President of Engineering, AWS. "Indeed, enabling cutting edge research in quantum computing and helping businesses prepare for the quantum future is why we launched Amazon Braket and built out our team of experts at the Amazon Quantum Solutions Lab. We're thrilled to support BMW and the quantum community in this innovation challenge. We applaud BMW's leadership in tackling real industrial challenges where quantum computers may one day provide an advantage."

BMW Group is driving the creation of a quantum ecosystem

The Quantum Computing Challenge once again underscores how the BMW Group is playing a leading role in efforts to establish a quantum ecosystem. As recently as June, the company joined forces with nine other major corporations to found the Quantum Technology and Application Consortium (QUTAC). The consortium's goal is to produce a high quantity of use cases for industry and, in so doing, create demand for quantum computing. QUTAC will speed up development of the technology in Germany and Europe.

On 16 June, the BMW Group, together with the Technical University of Munich (TUM), also announced the creation of an endowed chair in "Quantum Algorithms and Applications." Over a period of six years, the BMW Group will make a fund of €5.1 million available to TUM for a professorship, equipment and personnel. By taking this step, the BMW Group and TUM are seeking to bridge the gap between the outstanding basic research carried out in Germany and its specific application in industry.

33.Universal and operational benchmarking of quantum memories

by Xiao Yuan, Yunchao Liu, Qi Zhao, Bartosz Regula, Jayne Thompson & Mile Gu
https://www.nature.com/articles/s41534-021-00444-9

Quantum memory — the capacity to faithfully preserve quantum coherence and correlations — is essential for quantum-enhanced technology. There is thus a pressing need for operationally meaningful means to benchmark candidate memories across diverse physical platforms. Here we introduce a universal benchmark distinguished by its relevance across multiple key operational settings, exactly quantifying

(1) the memory's robustness to noise,
(2) the number of noiseless qubits needed for its synthesis,
(3) its potential to speed up statistical sampling tasks, and
(4) performance advantage in non-local games beyond classical limits.

The measure is analytically computable for low-dimensional systems and can be efficiently bounded in the experiment without tomography. We thus illustrate quantum memory as a meaningful resource, with our benchmark reflecting both its cost of creation and what it can accomplish. We demonstrate the benchmark on the five-qubit IBM Q hardware, and apply it to witness the efficacy of error-suppression techniques and quantify non-Markovian noise. We thus present an experimentally accessible, practically meaningful, and universally relevant quantifier of a memory's capability to preserve quantum advantage.

34.China tightens control over cybersecurity in data crackdown

by Joe McDonald
https://www.washingtonpost.com/business/china-tightens-control-over-cybersecurity-in-data-crackdown/2021/07/13/0b3bd7fe-e3da-11eb-88c5-4fd6382c47cb_story.html

Tech experts in China who find a weakness in computer security would be required to tell the government and couldn't sell that knowledge under rules further tightening the Communist Party's control over information.

The rules would ban private sector experts who find "zero day," or previously unknown security weaknesses, and sell the information to police, spy agencies or companies. Such vulnerabilities have been a feature of major hacking attacks including one this month blamed on a Russian-linked group that infected thousands of companies in at least 17 countries.

Beijing is increasingly sensitive about control over information about its people and economy. Companies are barred from storing data about Chinese customers outside China. Companies including ride-hailing service Didi Global Inc., which recently made its U.S. stock market debut, have been publicly warned to tighten data security.

Under the new rules, anyone in China who finds a vulnerability must tell the government, which will decide what repairs to make. No information can be given to "overseas organizations or individuals" other than the product's manufacturer.

No one may "collect, sell or publish information on network product security vulnerabilities," say the rules issued by the Cyberspace Administration of China and the police and industry ministries. They take effect Sept. 1.

The ruling party's military wing, the People's Liberation Army, is a leader along with the United States and Russia in cyber warfare technology. PLA officers have been charged by U.S. prosecutors with hacking American companies to steal technology and trade secrets.

Consultants that find "zero day" weaknesses say their work is legitimate because they serve police or intelligence agencies. Some have been accused of aiding governments accused of human rights abuses or groups that spy on activists.

There is no indication such private sector researchers work in China, but the decision to ban the field suggests Beijing sees it as a potential threat.

China has steadily tightened control over information and computer security over the past two decades.

Banks and other entities that are deemed sensitive are required to use only Chinese-made security products wherever possible. Foreign vendors that sell routers and some other network products in China are required to disclose to regulators how any encryption features work.

35.A bridge to post-quantum cryptography

by Iain Beveridge
https://blog2.entrust.com/blog/2021/07/a-bridge-to-post-quantum-cryptography/

The Tacoma Narrows suspension bridge- which spanned the Puget Sound in Washington state, USA – opened to the public in July 1940, and suffered a catastrophic collapse after only five months. This event had a profound effect on the fields of science and engineering. The bridge collapsed due to aeroelastic flutter, a type of self-sustaining structural oscillation that was not well understood at the time, and resulted in considerable research into the fields of aerodynamics and aeroelastics.

Fast forward 81 years and today we have another branch of science, quantum physics and its application in quantum computers – that is expected to be particularly disruptive in the field of cryptography. However, now we have ways of predicting the effects of quantum computers – before they can disrupt established cryptographic practices. This will allow us to be better prepared as we build new solutions that may impacted by advances in quantum computing.

The expectation is that quantum computing will render the strong cryptographic algorithms we use today ineffective through brute force attacks by dramatically speeding up the time it would take to break an encryption algorithm.

So what will the post-quantum world look like? There are a handful of theories, principles and algorithms you need to be familiar with – or at least be able to name drop into a conversation!

Shor's Algorithm

Postulated in 1994 by American mathematician Peter Shor, Shor's algorithm is a polynomial-time quantum computer algorithm yield exponential speedup when solving factoring. Large complex mathematical problems, like cryptographic algorithms, could thus be solved quickly using quantum computers – putting commonly used public-key cryptography schemes based on asymmetric algorithms such as RSA and elliptic curves at risk.

Grover's Algorithm

Grover's algorithm could weaken symmetric algorithms like AES. It suggests that an attacker with access to a quantum computer might be able to attack a symmetric cipher with a key up to twice as long as could be attacked with access only to standard computers. However, the National Institute for Standards and Technology (NIST) has considered Grover's algorithm and noted that, aside from the anticipated greater expense of quantum computing, to obtain the full quadratic speedup, all the steps of Grover's algorithm would have to be performed in series. This means that the 'speedup' might not be as impressive in comparison to massively parallel systems. NIST reports "it is quite

likely that Grover's algorithm will provide little or no advantage in attacking AES, and AES 128 will remain secure for decades to come." The full response from NIST can be read here.

Mosca's Theorem

Named for Canadian Michele Mosca, Mosca's theorem tackles the thorny topic of migration to a quantum safe ecosystem, and is designed to measure risk based on an organization's response to three questions:

(i) How long do you need your cryptographic keys to be remain secure? This is denoted as *x*, the security shelf life.

(ii) How long will it take to deploy a set of tools that are quantum-safe? This is denoted as *y*, the migration time.

(iii) How long will it be before a quantum computer, or some other method, breaks the currently deployed public-key cryptography tools? This is denoted as *z*, the collapse time.

Mosca expresses those questions in a simple formula determining if $x + y > z$ "we have a serious problem." It's worth exploring these ideas in detail.

Security Shelf life (*x*)

While some crypto keys in use today are ephemeral with a truly short life, many others, such as those used in public key infrastructure, need to be in use and secure for five, 10 or even 20 years or longer before it needs to be rotated. This is a non-trivial amount of time.

Another consideration is the "**store-now, decrypt later**" attack. A well-resourced attacker could target encrypted communications between two parties, and then hold the data for decryption when a quantum computer becomes available – this extends '*x*'

Migration Time (*y*)

Migration time isn't simply how long it takes for an organization to migrate their entire crypto ecosystem to quantum safe algorithms. It also needs to reflect the time for quantum safe algorithms to be established and fully accepted by industry and academics alike, reviewed, refined and thoroughly tested before being used real life situations. That can easily take 3-5 years. So adding *x* and *y* yields say worse-case scenario **(20 +5) 25** years.

Collapse Time (*z*)

Collapse time for the Tacoma Narrow's bridge was a mere five months – a disastrous turn of events. Academics and enterprise alike now speculate that quantum computers will have enough qubits to allow them to break the classic cryptographic algorithms in 15-20 years.

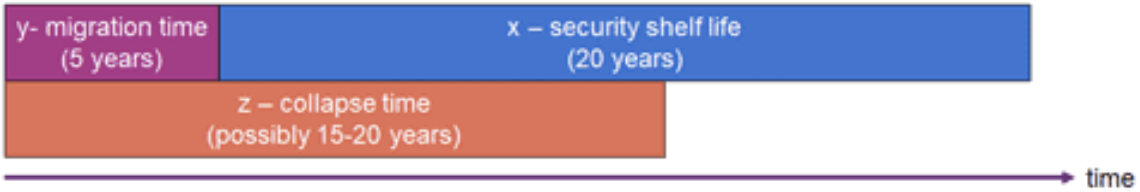


Figure 1: Illustration of Mosca's theorem

So back to the formula, as illustrated in figure 1, we have achieved $x + y > z$ — Houston we have a problem! Mosca's theorem serves as a stark reminder of why organizations need to start applying due diligence in the Post Quantum area now. NIST recently published a migration paper that serves as a statement of intent, outlining their plans to develop a set of tools that will in part address migration time (y). NIST is seeking comments from industry and academia, so if this is on your radar you can download the paper here.

Why Should I Care?

So you might be thinking, should this be keeping me awake at night? Are we facing a Tacoma Narrows situation? Predicting the collapse of classical cryptographic algorithms is currently very much in the crystal ball domain, but we do have time to plan and implement steps to make sure we are best prepared for when it happens. Fortunately, there is time to adopt some best practice steps:

- Ensure your organization has a Post Quantum Strategy in place. Lobby your Chief Security Officer to make it happen.
- Keep abreast of the emerging Post Quantum algorithms from NIST. Develop a plan to test and deploy them.
- Develop a crypto-agile mind set. Where possible, don't hardwire specific pre-quantum algorithms into your certificates and code. Make sure you have the ability to upgrade when required, adopting new Post Quantum algorithms as and when they become ratified.
- Until Post Quantum safe algorithms are available, use a hybrid approach of currently available Post Quantum resistant algorithms in conjunction with existing asymmetric algorithms.
- Use longer Symmetric keys and algorithms.

Right now, there is time to get ready. In a few years, that may not be the case. With these steps, you can get your organization on the right path to cross that bridge into a post quantum world.

36.Ransomware shows the power and weakness of the web

by Steve Ranger
https://www.zdnet.com/article/ransomware-shows-the-power-and-weakness-of-the-web/

Ransomware reflects the complexities and limitations of the web. It's worth remembering those limitations as we rely ever more on computer systems that often have pretty shallow foundations when it comes to security and reliability.

For example, much of the web has been built on trust, with security very much an after-thought. There's always been hacking, of course, but the difficulty of making it pay meant that, apart from state-sponsored attacks and industrial espionage, the impact was quite limited.

But the rise of cryptocurrency, which enables hard-to-track payments, plus the general insecurity of many computer systems, and our total reliance on them, has created the perfect ransomware storm that now engulfs so many companies.

Fixing this problem is not easy. The US administration may now be threatening to take action against ransomware gangs, but because many of them operate from Russia, that's going to be tough.

True, the US could try to break the infrastructure that the gangs use, but that's not without its problems. For a start, these gangs don't have huge infrastructure to attack, and what they do have is easily replaced. Then there's the risk of accidentally disrupting the systems of an innocent organisation in a foreign country, which -- particularly when you're dealing with Russia -- is a good way to raise international tensions.

Most likely the US could try to put a tight financial squeeze on ransomware gangs -- something it has already done by seizing some of the bitcoins sent to them. These gangs are entirely motivated by money, so taking away the ability to receive ransoms or spend their ill-gotten gains is likely to be the most effective way of curtailing their activities. Banning the payment of ransoms might have some impact, but it would also force some unlucky firms out of business if their data was locked up forever.

The ransomware era will probably come to an end at some point, most likely to be replaced with another security worry. Indeed, the rise of supply chain security flaws, which are currently being exploited to spread ransomware, is at least as big a problem.

But the ransomware problem also serves as a reminder: we are increasingly reliant on the web, and the internet beneath it. And much of that infrastructure is creaking, or held in place by obscure but fragile systems or pieces of code. So even after ransomware is long forgotten, the security worries won't go away.

37.Quantum computing: This new 100-qubit processor is built with atoms cooled down near to absolute zero

by Daphne Leprince-Ringuet
https://www.zdnet.com/article/quantum-computing-this-new-100-qubit-processor-is-built-with-atoms-cooled-down-near-to-absolute-zero/?utm_medium=email&_hsmi=144433981&_hsenc=p2ANqtz-_H_Sx4_7o0AXw-XjH0HnPuDV-Tl7Zsa9NVGM5kBH4SSQUbs05zDdwH_yCFMkSfcr0v__kpf-QH7Syuy8f89g11wqzN_yhQ&utm_content=144433981&utm_source=hs_email

By cooling atoms down to near absolute zero and then controlling them with lasers, a company has successfully created a 100-qubit quantum processor that compares to the systems developed by leading quantum players to date.

ColdQuanta, a US-based company that specializes in the manipulation of cold atoms, unveiled the new quantum processor unit, which will form the basis of the company's 100-qubit gate-based quantum computer, code-named **Hilbert**, launching later this year after final tuning and optimization work.

There are various different approaches to quantum computing, and among those that have risen to prominence in the last few years feature superconducting systems, trapped ions, photonic quantum computers and even silicon spin qubits.

Cold atoms, on the other hand, haven't made waves in the quantum ecosystem so far. ColdQuanta's 100-qubit quantum processor, however, could seemingly compete against the industry's highest standards: for example, IBM's current quantum system, Hummingbird, supports 65 qubits.

And in the next three years, **ColdQuanta is hoping to create a system surpassing 1,000 qubits**. This again aligns with IBM's roadmap for quantum hardware, which should see the company releasing a 1,121-qubit quantum computer in 2023.

"We hear a lot about superconducting and trapped ions and in some respects cold atom is the new kid on the block, but we believe it has great promise in terms of scalability," Paul Lipman, president of quantum computing at ColdQuanta, tells ZDNet.

ColdQuanta's approach consists of treating atoms like qubits, and bringing them down to extremely cold temperatures, where their quantum properties can be manipulated with great precision. This is because, in such an isolated environment, atoms are protected from environmental noise and can retain their quantum properties for much longer.

Cooling down particles to exert better control over them is not new to the quantum world: Google and IBM's superconducting processors also require placing qubits in huge dilution refrigerators, where temperatures are brought down to zero kelvin (-273.15C).

But ColdQuanta's cold atoms approach goes one step further. Atoms are cooled down to the microkelvin level – that is, a thousand times colder than in the superconducting method.

Rather than using large refrigerators, however, ColdQuanta traps the atoms with lasers to cool them down, before using a combination of lasers and microwave pulses to arrange them into the gates that make up a quantum circuit.

"Because we cool them down with lasers rather than dilution refrigerators, we don't have the same scaling challenges in terms of building enormous fridges that can hold large numbers of qubits," says Lipman. "We cool them down to microkelvin, but we do that in a device that can fit in your hand at room temperature."

What's more: atoms are ten-thousand times smaller than superconducting qubits, according to Lipman, meaning that many cold atom qubits can be packed closely together on a much smaller space. What would require square-meters worth of space for a superconducting quantum processor can sit on a cold atom system the size of a nail, according to the company.

"Cold atoms have this intrinsic scalability that is very attractive," argues Lipman.

Cold atoms' ability to scale rapidly is one of ColdQuanta's key selling points, but there remain some engineering challenges that, for now, still limit Hilbert's size. The company's scientists are looking at how the use of lasers changes when the qubit count increases by orders of magnitude, for instance, and testbeds are already underway in the lab to determine the best path forward.

The fundamental principles of the approach, however, are tested and proven, says Lipman, and cold atoms already perform similarly to leading-edge quantum processors. Not only on qubit count: the company's data also shows that the system is comparable to IBM and Google's quantum computers when it comes to connectivity, which refers

to the number of qubits that can interact with one another, and coherence, which is the duration of time that quantum properties can be maintained.

On fidelity, however, the processor lags slightly behind the devices developed by competitors, meaning that the accuracy of ColdQuanta's system isn't as high. But part of the optimization work going on now, says Lipman, is dedicated to boosting Hilbert's performance on fidelity.

Lipman is confident that these promising results will set ColdQuanta apart in an ecosystem that is growing at pace. New milestones are announced by quantum companies large and small at a rapid pace, and the number of approaches to quantum computing is multiplying fast, each with their own benefits and challenges – making it increasingly difficult to distinguish hype from reality.

"It's too early to tell which modality will win the race," admits Lipman. "If you roll the clock forward two or three years, there might even be modalities that we don't even have publicly available information on today, but may come to the forefront."

"We'll learn more once the computer is released, but our focus now is to work with potential customers to deliver tangible near-term value."

ColdQuanta has not publicly announced any customers yet, but the company is working particularly on optimization problems, which could find applications in logistics, material science and telecommunications.

The firm also has a long-standing partnership with the Defense Advanced Research Projects Agency (DARPA), which awarded ColdQuanta a total $7.4 million to develop a scalable cold-atom-based quantum computer for defense applications such as resource allocation, logistics, and image recognition.

Hilbert is expected to launch later this year and will be available over ColdQuanta's private cloud. The company is also in talks with Amazon, Microsoft and Google to eventually make the quantum computer accessible over AWS, Azure and Google Cloud.

38.How quantum networking could transform the internet

by Scott Fulton III
https://www.zdnet.com/article/could-quantum-networking-rescue-the-communications-industry-status-report/

Quantum computing (QC) and quantum networking (QN) are related, though independent, industries. Both leverage the same unexplained phenomenon in quantum physics: the entanglement between particles that enables them to share states -- or in the digital sense, information -- in apparent violation of relativity theory. But as services, they fulfill separate functions.

QC endeavors to solve problems typically delegated to supercomputers, or that would be so delegated if supercomputers were fast enough to resolve those problems within our lifetimes.

QN would secure connections between digital devices (including the conventional variety -- yours and mine) using a physics technique that would be permanently crack-proof. It would rather let the connection crash than allow it to be pilfered.

In a previous *Status Report* published in March, I came down hard on quantum computing as a viable technology. I had just taken part in a virtual quantum conference where QC and QN were both featured on the same stage. And I came away with a single, conglomerate viewpoint about the two endeavors. If you read my ZDNet colleague Daphne Prince-Ringuet's thorough, up-to-date coverage, you might wonder from whence my negative attitude about QC sprang forth (not quite iambic pentameter, but I tried).

As some folks have kindly told me, there's a completely different business model for the first startups and the established cloud players building quantum computers compared with the academics and security professionals experimenting with quantum networks. The latter would, at the very least, revolutionize cybersecurity. At most, it could force a cataclysmic change in the way the entire Internet is operated. If no conventional cryptography can possibly avoid a near-instantaneous crack by a QC system, theoretically, HTTPS as a protocol would become pointless.

With this edition of *Status Report*, we'll update our view of QC and add an independent assessment of QN. Here's how these assessments work: For each topic, we look at 10 categories of influence, rating each of their progressive and regressive potentials on positive-10 and negative-10-point scales, respectively. Then on a 2D Cartesian chart, we give each category its own compass direction or *vector*, plot the position of each influence point on that vector and compute the geometric average location of all points. The distance of that average point from the dead center is our final influence score.

39.How to prevent ransomware attacks with a zero-trust security model

by Scott Matteson
https://www.techrepublic.com/article/how-to-prevent-ransomware-attacks-with-a-zero-trust-security-model/

Ransomware attacks take place 4,000 times worldwide every day. The process is fairly straightforward—malware infects a target computer, and an attacker encrypts valuable data then sends the victim a notification demanding a ransom payment to release access to it. It's a gamble: If the ransom is paid there is no guarantee the attacker will release the data.

It's worth pointing out this is a real phenomenon which actually locks up targeted data; it's not the same as a random email from a stranger stating they "have gained access to your devices, which you use for internet browsing" and "after that, I have started tracking your internet activities" whereby they proceed to accuse you of engaging in unsavory online behavior which they threaten to expose unless you send them Bitcoin. Those are safe to ignore. Ransomware cannot be ignored.

TechRepublic has offered many tips on combatting ransomware as well as strategies for being proactive about it. However, there is a zero-trust model to cybersecurity that can also help businesses stay secure.

Duncan Greatwood, CEO of Xage, a zero-trust security company, pointed out that a ransomware attack can be much more damaging than just preventing access to valuable data. That's an inconvenience and a potential disruption to business operations, but when an energy or utility grid is compromised, this can lead to blackouts, gridlocks and—when safety mechanisms are breached—the release of toxic chemicals, oil spills, fires or explosions.

Furthermore, Greatwood pointed out, wealthy countries and businesses are prime targets for ransomware attacks. "The higher the expectation for service reliability, quality and trust, the more likely the business will be a target of the attack. For these companies the impact due to loss of revenue and reputation is much greater than the payout. They also have the working capital to pay the ransom. Utilities, oil and gas operators, pipelines, chemical manufacturing, and the food and beverage industry are prime targets," he said.

The problem is exacerbated by the fact that as of late the skills required to execute a ransomware attack have been dramatically reduced. "Ransomware software packages exist along with millions of stolen access credentials on the dark web that allow people with relatively little technical background to effectively execute ransomware attacks. In fact, ransomware-as-a-service models are emerging with complete software offerings for hackers. Hacker groups are based all over the world with some concentration in Eastern Europe, China, Iran, Russia," Greatwood said.

Identity-based access, frequent password changes and multi-factor authentication can help reduce the incidence of such attacks, but to be proactive Greatwood and I agreed that identifying the source of repeated, excessive login attempts and blocking such attempts are crucial to detecting and reducing the impact of ransomware attacks.

A zero-trust model is a valuable defense mechanism in blocking ransomware. "One of the most effective ways to prevent ransomware attacks is through the adoption of zero-trust architecture, the modern alternative to perimeter-based security. Built on the principle 'never trust, always verify,' a zero-trust security strategy would have prevented ransomware attacks like the Colonial Pipeline and JBS, by preventing it from spreading across the operations while keeping the operation running.

The Colonial Pipeline attack as well as many other recent attacks (JBS, Brenntag, Oldsmar, etc.) demonstrate that industrial operations lack the security controls across their operation to effectively identify, isolate and recover infected systems. Cybersecurity controls across the operations gives the operator the ability to control each interaction between applications, users and machines on an individual basis based on the identity and policy and with zero trust. When such controls exist they give the operator a method to prevent the attack from spreading and the operation can keep running even during an active attack," Greatwood said.

"Unlike traditional techniques, under which an attacker can exploit cyber weaknesses upon gaining access inside a network segment perimeter, zero trust treats the identity of each machine, application, user and data stream as its own independent 'perimeter,' allowing granular access policy enforcement. As such, rigorous security enforcement continues even in the event that hackers get into an operational or corporate network—and ransomware gets blocked from traversing between IT and OT systems," Greatwood said.

Greatwood also emphasized that zero trust is especially crucial for companies in industries that have been slower to modernize, such as oil and gas, utilities, and energy. Due to their delayed digital transformation, as well as a mix of legacy and modern equipment, these companies are often the most difficult to secure.

"Cybersecurity and Infrastructure Security Agency recently published a set of guidelines specifically for industrial operations due to the rise of ransomware attacks in this sector. National Institute of Standards and Technology has also been updating its set of guidelines for protecting Industrial Control Systems from such attacks. Both are advocating for a defense-in-depth approach focusing on zero-trust with granular role-based access management for all interactions in the OT and especially in IT/Cloud environments," Greatwood said."

"Zero trust really means a way to control interactions between users, machines, apps and even data on an individual basis requiring authentication and authorization per security policy, vertically and horizontally and across multiple levels. Organizations need to implement controls throughout their environments—cloud, enterprise, control center, facilities, substations, wind farms, everywhere to be able to not only protect, but also quickly isolate infested systems, and recover operations," he added.

Here are the benefits (and requirements) of a distributed zero-trust cybersecurity system (cybersecurity mesh/fabric) as laid out by Greatwood:

- No reliance on implicit trust zones, static accounts and firewall rules
- Each identity (user, machine, app, data) forms its own perimeter protection
- Access permissions controlled based on identity, role and policy
- All interactions have “just-enough-access” enabled “just-in-time"
- Unsecured protocols such as RDP, VNC, Modbus and their vulnerabilities are never exposed outside of the organization, instead proxied over TLS sessions
- Unlike VPNs that put remote user devices (and potential malware on them) into networks, ZTA remote user devices are never inside the network (not even corporate)
- Controls user-to-machine, machine-to-machine, app-to-machine, and app-to-data interactions and secures file and data transfer within and across OT, IT and Cloud
- Vertical (corporate and remote to control network) and horizontal (ICS site-to-site) access management
- Driven by central policy management and enforced using distributed nodes (any asset, any location). The cybersecurity mesh with distributed identity-based enforcement is a top strategic trend for 2021, according to Gartner.
- Overlays into existing OT/IT architectures with no network changes or systems changes (compatible with existing deployed base of workstations, HMIs, IEDs, etc.)

Greatwood pointed out the risk of liability here: “Companies paying ransomware fees — the victims of ransomware — may also be exposing themselves to serious legal risk depending on the identity and origin of the hackers, since U.S. laws prohibit sending funds to certain organizations and people, such as terrorists or some organized-crime syndicates, and also prohibits companies from doing business with certain countries."

40.ADVA launches world’s first optical transport solution with post-quantum cryptography

by ADVA
https://www.businesswire.com/news/home/20210708005050/en/ADVA-launches-world%E2%80%99s-first-optical-transport-solution-with-post-quantum-cryptography

ADVA today launched the industry’s first optical transport solution secured by post-quantum cryptography (PQC). The FSP 3000 ConnectGuard™ optical encryption solution now protects data against cyberattacks from quantum computers that could break today’s cryptographic algorithms. The quantum-safe security technology relies on a hybrid key exchange system, combining PQC algorithms with classical encryption methods. Built for crypto-agility,

the solution is ready for software updates in the future, ensuring it delivers the most robust network protection now and for decades to come.

“Our market-first FSP 3000 quantum-safe ConnectGuard™ encryption technology answers the urgent threat posed by quantum computers and gives organizations a way to safeguard their networks before the danger materializes. Our customers’ data will be fully protected even from cybercriminals’ intent on harvesting information so that they can store it today and exploit it tomorrow,” said Christoph Glingener, CTO, ADVA. “We’re providing long-term security for data in motion. What’s more, our solution is ready to be upgraded later to comply with emerging specifications, including the NIST’s PQC standardization competition.”

As recommended by leading cybersecurity authorities, the PQC-protected ADVA FSP 3000 ConnectGuard™ encryption solution **utilizes the traditional Diffie-Hellman protocol and combines it with a newly developed algorithm based on the quantum-safe McEliece cryptosystem**. This enables it to produce encryption keys that even powerful quantum computers will be unable to crack. As well as delivering data integrity with quantum-safe Layer 1 AES-256 protection, the ADVA FSP 3000 ConnectGuard™ encryption solution ensures minimal impact on latency, throughput and performance. The technology is also easily deployable over long-haul and multi-operator links.

“Organizations everywhere have woken up to the security threat that quantum computing represents. With many experts anticipating powerful commercially available quantum computers in the next decade, it’s now widely understood that the danger is very real and the stakes are enormously high. That’s why we’ve invested so much time and energy into developing the world’s first transport solution ready for the challenges ahead,” commented Jörg-Peter Elbers, SVP, advanced technology, ADVA. “By integrating PQC security into our FSP 3000 ConnectGuard™ optical encryption solution, we’re empowering our customers to protect their networks today against tomorrow’s threats. Our solution is easily deployable and only requires end-point access. What’s more, it works over any distance and in any optical transport network.”

41.Terra Quantum announces 40,000km quantum cryptography breakthrough

by MAIJA PALMER
https://sifted.eu/articles/40000km-quantum-cryptography-breakthrough/

Terra Quantum, the Swiss quantum technology company, is today announcing a breakthrough in quantum cryptography with a technology that allows quantum cryptography keys to be transmitted over a distance of more than 40,000km — the circumference of the Earth.

It blows all previous quantum cryptography distance records out of the water with an almost 100x improvement and potentially solves the biggest problem preventing quantum cryptography from becoming practically usable.

The world faces a huge threat in the next few years when quantum computers become powerful enough to break the cryptography of conventional computers. Everything from government communications to the contents of Bitcoin wallets would become vulnerable to hackers.

“We’re not talking in 10 years, it will be within 2 to 5 years,” says Markus Pflitsch, founder and CEO of Terra Quantum. Hackers and hostile governments are likely to be among the first to harness quantum computers for code-breaking and the computer industry is becoming acutely aware that it needs to find ways to protect itself.

Quantum cryptography is one of the best solutions — in theory, the laws of physics make a network linked by quantum connections unhackable. In practice, there is a big problem: quantum key distribution only works over relatively short distances. Photons, which are used for these transmissions, get scattered or absorbed along the route. Record distances for quantum key distribution so far have been 421km (in 2018), and a Chinese research group last year took this to 509km.

In order to send a secure quantum key between, say, London and New York (5,567km) to secure a stock market trade, you'd need to put multiple repeaters into the line to boost the signal. Each one of these repeaters becomes a potential point of vulnerability, where the signal can be intercepted. So quantum cryptography developers have been trying to find ways to do without these.

Some companies are trying to solve this by building new networks — UK-based Arqit, which recently announced plans to go public via a $1.4bn SPAC, for example, is planning to use satellites to distribute secure quantum cryptography keys. But this infrastructure will take time to put in place. One big advantage of Terra Quantum's solution is that it can run inside a standard optical fibre line, already in use today in telecoms networks.

The technology is based on measuring the loss of photons over a particular line and carefully controlling the transmitted signal so that the amount of signal that an eavesdropper on the line is never enough to be able to extract meaningful information.

"We can know exactly how much of the signal is being intercepted and can tweak it to make sure that the eavesdropper only gets a few photons — which would be obscured by quantum noise," says Nikita Kirsanov, project lead at Terra Quantum.

The technique is based around the second law of thermodynamics — the one that states that entropy always increases and a more detailed academic paper published here.

But Pflitsch is keen to stress that the technology is not in the realms of academic papers. Terra Quantum is in talks with several telecoms companies to run proof of concept projects to demonstrate the system. "This is not something for the future, we can do this today," he said.

42.Narrowing the gap between theory and practice for quantum secure communications

by Sam Jarman

https://www.quantumlah.org/about/highlight/2021-07-qkd-power-limiter

Researchers from CQT and their collaborators have developed two methods, one theoretical and one experimental, to protect the security of quantum key distribution (QKD), a technology that can be deployed in any communication network that needs long-term security. The first is a twist on the ultra-secure cryptography protocol known as '**device-independent' QKD (DIQKD)**. The second is a first-of-its-kind device that defends QKD systems against bright light pulse attacks by creating a power threshold.

QKD is a method for secure communication that uses quantum mechanics to encrypt information. While the security of QKD is unbreakable in principle, if it is incorrectly implemented, vital information could still be stolen by attackers. These are known as side-channel attacks, where the attackers exploit weaknesses in the setup of the information system to eavesdrop on the exchange of secret keys. The two new methods proposed ensure that QKD communications cannot be attacked in this way.

"Rapid advances in quantum computing and algorithmic research mean we can no longer take today's toughest security software for granted. Our two new approaches hold promise to ensuring that the information systems which we use for banking, health and other critical infrastructure and data storage can hold up any potential future attacks," said CQT Principal Investigator Charles Lim, who led the two research projects. Charles holds a joint appointment as Assistant Professor in the NUS Department of Electrical and Computer Engineering.

Future-proof quantum communication protocol

Critically, the security of DIQKD can be checked without needing to characterise the quantum devices uses. Typically, in QKD, quantum devices perform measurements using two measurement settings – one to make a secret key and another to test the integrity of the channel.

In a paper published in *Nature Communications* on 17 May 2021, the team showed that with their new DIQKD protocol, users can independently test the other party's encryption device by generating a secret key from two randomly chosen key generation settings instead of one. The researchers demonstrated that introducing an extra set of key-generating measurement for the users makes it harder for the eavesdropper to steal information.

"It's a simple variation of the original protocol that started this field, but it can only be tackled now thanks to significant developments in mathematical tools," says CQT Principal Investigator Valerio Scarani, who was one of the inventors of this type of method and is a co-author on the paper. Besides Charles, the other co-authors are René Schwonnek and Goh Koon Tong from NUS, Ignatius William Primaatmaja from CQT, Ernest Tan from ETH Zürich and Ramona Wolf from Leibniz Universität Hannover.

Compared to the original DIQKD protocol, the new protocol is easier to set up, and is more tolerant to noise and loss. It also gives users the highest level of security allowable by quantum communications and empowers them to independently verify their own key generation devices.

With the team's setup, all information systems built with DIQKD would be free from misconfiguration and mis-implementation. "Our method allows data to be safe against attackers even if they have unlimited quantum computing power. This approach could lead to a truly secure information system, eliminating all side-channel attacks and allowing end-users to monitor its implementation security easily and with confidence," explained Charles.

A first-of-its-kind quantum power limiter device

Quantum cryptography, in practice, uses optical pulses with very low light intensity to exchange data over untrusted networks. Leveraging quantum effects can securely distribute secret keys, generate truly random numbers, and even create banknotes that are mathematically unforgeable.

However, experiments have shown that it is possible to inject bright light pulses into the quantum cryptosystem to break its security. This side-channel attack strategy exploits the way injected bright light is reflected to the outside environment, to reveal the secrets being kept in the quantum cryptosystem.

In a new paper published in *PRX Quantum* on 7 July 2021, the researchers from CQT and NUS reported their development of the first optical device to address the issue. Zhang Gong, Wang Chao, Haw Jing Yan and Gong Xiao from the NUS Department of Electrical and Computer Engineering worked on this project with Charles and Ignatius.

The optical device is based on thermo-optical defocusing effects to limit the energy of the incoming light. The researchers use the fact that the energy of the bright light changes the refractive index of the transparent plastic material embedded in the device, thus it sends a fraction of the light out of the quantum channel. This enforces a power limiting threshold.

The team's power limiter can be seen as an optical equivalent of an electric fuse, except that it is reversible and does not burn when the energy threshold is breached. It is highly cost-effective, and can be easily manufactured with off-the-shelf components. It also does not require any power, so it can be easily added to any quantum cryptography system to strengthen its implementation security.

Charles added, "It is imperative to close the gap between the theory and practice of quantum secure communications if we are to use it for the future Quantum Internet. We do this holistically – on one hand we design more practical quantum protocols and on the other hand, we engineer quantum devices that conform closely with the mathematical models assumed by the protocols. In doing so, we can significantly narrow the gap."

43.How Does a Quantum Computer Work?

by Michael Tabb, Andrea Gawrylewski, Jeffery DelViscio
https://www.scientificamerican.com/video/how-does-a-quantum-computer-work/

If someone asked you to picture a quantum computer, what would you see in your mind?

Maybe you see a normal computer-- just bigger, with some mysterious physics magic going on inside? Forget laptops or desktops. Forget computer server farms. A quantum computer is fundamentally different in both the way it looks, and, more importantly, in the way it processes information.

There are currently several ways to build a quantum computer. But let's start by describing one of the leading designs to help explain how it works.

Imagine a lightbulb filament, hanging upside down, but it's the most complicated light you've ever seen. Instead of one slender twist of wire, it has organized silvery swarms of them, neatly braided around a core. They are arranged in layers that narrow as you move down. Golden plates separate the structure into sections.

The outer part of this vessel is called the chandelier. It's a supercharged refrigerator that uses a special liquified helium mix to cool the computer's quantum chip down to near absolute zero. That's the coldest temperature theoretically possible.

At such low temperatures, the tiny superconducting circuits in the chip take on their quantum properties. And it's those properties, as we'll soon see, that could be harnessed to perform computational tasks that would be practically impossible on a classical computer.

Traditional computer processors work in binary—the billions of transistors that handle information on your laptop or smartphone are either on (1) or they're off (0). Using a series of circuits, called "gates," computers perform logical operations based on the state of those switches.

Classical computers are designed to follow specific inflexible rules. This makes them extremely reliable, but it also makes them ill-suited for solving certain kinds of problems—in particular, problems where you're trying to find a needle in a haystack.

This is where quantum computers shine.

If you think of a computer solving a problem as a mouse running through a maze, a classical computer finds its way through by trying every path until it reaches the end.

What if, instead of solving the maze through trial and error, you could consider all possible routes simultaneously?

Quantum computers do this by substituting the binary "bits" of classical computing with something called "qubits." Qubits operate according to the mysterious laws of quantum mechanics: the theory that physics works differently at the atomic and subatomic scale.

The classic way to demonstrate quantum mechanics is by shining a light through a barrier with two slits. Some light goes through the top slit, some the bottom, and the light waves knock into each other to create an interference pattern.

But now dim the light until you're firing individual photons one by one—elementary particles that comprise light. Logically, each photon has to travel through a single slit, and they've got nothing to interfere with. But somehow, you still end up with an interference pattern.

Here's what happens according to quantum mechanics: Until you detect them on the screen, each photon exists in a state called "superposition." It's as though it's traveling all possible paths at once. That is, until the superposition state "collapses" under observation to reveal a single point on the screen.

Qubits use this ability to do very efficient calculations.

For the maze example, the superposition state would contain all the possible routes. And then you'd have to collapse the state of superposition to reveal the likeliest path to the cheese.

Just like you add more transistors to extend the capabilities of your classical computer, you add more qubits to create a more powerful quantum computer.

Thanks to a quantum mechanical property called "entanglement," scientists can push multiple qubits into the same state, even if the qubits aren't in contact with each other. And while individual qubits exist in a superposition of two states, this increases exponentially as you entangle more qubits with each other. So a two-qubit system stores 4 possible values, a 20-qubit system more than a million.

So what does that mean for computing power? It helps to think about applying quantum computing to a real world problem: the one of prime numbers.

A prime number is a natural number greater than 1 that can only be divided evenly by itself or 1.

While it's easy to multiply small numbers into giant ones, it's much harder to go the reverse direction; you can't just look at a number and tell its factors. This is the basis for one of the most popular forms of data encryption, called RSA.

You can only decrypt RSA security by factoring the product of two prime numbers. Each prime factor is typically hundreds of digits long, and they serve as unique keys to a problem that's effectively unsolvable without knowing the answers in advance.

In 1995, M.I.T. mathematician Peter Shor, then at AT&T Bell Laboratories, devised a novel algorithm for factoring prime numbers whatever the size. One day, a quantum computer could use its computational power, and Shor's algorithm, to hack everything from your bank records to your personal files.

In 2001, IBM made a quantum computer with seven qubits to demonstrate Shor's algorithm. For qubits, they used atomic nuclei, which have two different spin states that can be controlled through radio frequency pulses.

This wasn't a great way to make a quantum computer, because it's very hard to scale up. But it did manage to run Shor's algorithm and factor 15 into 3 and 5. Hardly an impressive calculation, but still a major achievement in simply proving the algorithm works in practice.

Even now, experts are still trying to get quantum computers to work well enough to best classical supercomputers.

That remains extremely challenging, mostly because quantum states are fragile. It's hard to completely stop qubits from interacting with their outside environment, even with precise lasers in supercooled or vacuum chambers.

Any noise in the system leads to a state called "decoherence," where superposition breaks down and the computer loses information.

A small amount of error is natural in quantum computing, because we're dealing in probabilities rather than the strict rules of binary. But decoherence often introduces so much noise that it obscures the result.

When one qubit goes into a state of decoherence, the entanglement that enables the entire system breaks down.

So how do you fix this? The answer is called error correction--and it can happen in a few ways.

> **Error Correction #1:** A fully error-corrected quantum computer could handle common errors like "bit flips," where a qubit suddenly changes to the wrong state.
>
> To do this you would need to build a quantum computer with a few so-called "logical" qubits that actually do the math, and a bunch of standard qubits that correct for errors.
>
> It would take a lot of error-correcting qubits—maybe 100 or so per logical qubit--to make the system work. But the end result would be an extremely reliable and generally useful quantum computer.
>
> **Error Correction #2:** Other experts are trying to find clever ways to see through the noise generated by different errors. They are trying to build what they call "Noisy intermediate-scale quantum computers" using another set of algorithms.
>
> That may work in some cases, but probably not across the board.
>
> **Error Correction #3:** Another tactic is to find a new qubit source that isn't as susceptible to noise, such as "topological particles" that are better at retaining information. But some of these exotic particles (or quasiparticles) are purely hypothetical, so this technology could be years or decades off.

> Because of these difficulties, quantum computing has advanced slowly, though there have been some significant achievements.

In 2019, Google used a 54-qubit quantum computer named "Sycamore" to do an incredibly complex (if useless) simulation in under 4 minutes—running a quantum random number generator a million times to sample the likelihood of different results.

Sycamore works very differently from the quantum computer that IBM built to demonstrate Shor's algorithm. Sycamore takes superconducting circuits and cools them to such low temperatures that the electrical current starts to behave like a quantum mechanical system. At present, this is one of the leading methods for building a quantum computer, alongside trapping ions in electric fields, where different energy levels similarly represent different qubit states.

Sycamore was a major breakthrough, though many engineers disagree exactly how major. Google said it was the first demonstration of so-called quantum advantage: achieving a task that would have been impossible for a classical computer.

It said the world's best supercomputer would have needed 10,000 years to do the same task. IBM has disputed that claim.

At least for now, serious quantum computers are a ways off. But with billions of dollars of investment from governments and the world's biggest companies, the race for quantum computing capabilities is well underway. The real question is: how will quantum computing change what a "computer" actually means to us. How will it change how our electronically connected world works? And when?

44.Quantum computer is smallest ever, claim physicists

by Sam Jarman

https://physicsworld.com/a/quantum-computer-is-smallest-ever-claim-physicists/

The smallest quantum computer to date has been claimed by a team of researchers in Austria, Switzerland, and Germany. Using strings of trapped ions that are addressed using laser pulses, Ivan Pogorelov at the University of Innsbruck and colleagues created a system that contains 24 fully-entangled quantum bits (qubits) and is housed in two industry-standard server racks.

The teams says that the computer's performance matches that of existing state-of-the-art systems and believe that their setup could bring the widespread use of practical quantum computers a step closer to reality.

As technology improves, quantum computers are integrating increasing numbers of qubits with the goal of creating devices that can solve certain problems much faster than conventional computers. Existing ways of integrating qubits often require a room full of equipment so researchers have now turned their attention to developing much more compact and practical implementations. These efforts face numerous challenges, however, including how to reliably manufacture large numbers of identical qubits and how to maintain the quantum coherence of qubits during complex operations such as the quantum entanglement of ions.

Calcium ions

Pogorelov and colleagues tackled these challenges in a system that uses entangled calcium ions as qubits. The ions are held in place within a Paul trap, which confines charged particles using dynamic electric fields. Within the trap, the entanglement of up to 50 ions can be achieved through interactions with laser pulses, which are also used to read out and write quantum information onto individual ions.

The team's setup was compact enough to be implemented within several modules that occupy two industry-standard server racks. Contained within aluminium boxes, the stackable modules include all the electrical components needed to generate and control the laser light and all necessary components for communication and remote control.

As an initial demonstration, the team used the setup to create a Greenberger-Horne-Zeilinger state that contained up to 24 fully entangled qubits. During this operation, the ions retained their quantum information without any need for error mitigation techniques – matching the performance of much larger state-of-the-art implementations.

The team says that the modular system has high mechanical stability, easily replaceable parts, and minimal requirements for system maintenance. They say that the system can be operated by trained non-specialists and that it could also be used by people worldwide via cloud-based quantum computing. Pogorelov and colleagues are now making further improvements to their system with the aim of achieving the full entanglement of all 50 qubits trapped within the ion string.

The system is described in *PRX Quantum*.

45.Harvard-led physicists take big step in race to quantum computing

by Juan Siliezar
https://news.harvard.edu/gazette/story/2021/07/harvard-led-physicists-create-256-qubit-programmable-quantum-simulator/

A team of physicists from the Harvard-MIT Center for Ultracold Atoms and other universities has developed a special type of quantum computer known as a **programmable quantum simulator capable of operating with 256 quantum bits**, or "qubits."

The system marks a major step toward building large-scale quantum machines that could be used to shed light on a host of complex quantum processes and eventually help bring about real-world breakthroughs in material science, communication technologies, finance, and many other fields, overcoming research hurdles that are beyond the capabilities of even the fastest supercomputers today. Qubits are the fundamental building blocks on which quantum computers run and the source of their massive processing power.

"This moves the field into a new domain where no one has ever been to thus far," said Mikhail Lukin, the George Vasmer Leverett Professor of Physics, co-director of the Harvard Quantum Initiative, and one of the senior authors of the study published today in the journal Nature. "We are entering a completely new part of the quantum world."

According to Sepehr Ebadi, a physics student in the Graduate School of Arts and Sciences and the study's lead author, it is the combination of system's unprecedented size and programmability that puts it at the cutting edge of the

race for a quantum computer, which harnesses the mysterious properties of matter at extremely small scales to greatly advance processing power. Under the right circumstances, the increase in qubits means the system can store and process exponentially more information than the classical bits on which standard computers run.

“The number of quantum states that are possible with only 256 qubits exceeds the number of atoms in the solar system,” Ebadi said, explaining the system’s vast size.

Already, the simulator has allowed researchers to observe several exotic quantum states of matter that had never before been realized experimentally, and to perform a quantum phase transition study so precise that it serves as the textbook example of how magnetism works at the quantum level.

These experiments provide powerful insights on the quantum physics underlying material properties and can help show scientists how to design new materials with exotic properties.

The project uses a significantly upgraded version of a platform the researchers developed in 2017, which was capable of reaching a size of 51 qubits. That older system allowed the researchers to capture ultra-cold rubidium atoms and arrange them in a specific order using a one-dimensional array of individually focused laser beams called optical tweezers.

This new system allows the atoms to be assembled in two-dimensional arrays of optical tweezers. This increases the achievable system size from 51 to 256 qubits. Using the tweezers, researchers can arrange the atoms in defect-free patterns and create programmable shapes like square, honeycomb, or triangular lattices to engineer different interactions between the qubits.

“The workhorse of this new platform is a device called the spatial light modulator, which is used to shape an optical wavefront to produce hundreds of individually focused optical tweezer beams,” said Ebadi. “These devices are essentially the same as what is used inside a computer projector to display images on a screen, but we have adapted them to be a critical component of our quantum simulator.”

The initial loading of the atoms into the optical tweezers is random, and the researchers must move the atoms around to arrange them into their target geometries. The researchers use a second set of moving optical tweezers to drag the atoms to their desired locations, eliminating the initial randomness. Lasers give the researchers complete control over the positioning of the atomic qubits and their coherent quantum manipulation.

Other senior authors of the study include Harvard Professors Subir Sachdev and Markus Greiner, who worked on the project along with Massachusetts Institute of Technology Professor Vladan Vuletić, and scientists from Stanford, the University of California Berkeley, the University of Innsbruck in Austria, the Austrian Academy of Sciences, and QuEra Computing Inc. in Boston.

“Our work is part of a really intense, high-visibility global race to build bigger and better quantum computers,” said Tout Wang, a research associate in physics at Harvard and one of the paper’s authors. “The overall effort [beyond our own] has top academic research institutions involved and major private-sector investment from Google, IBM, Amazon, and many others.”

The researchers are currently working to improve the system by improving laser control over qubits and making the system more programmable. They are also actively exploring how the system can be used for new applications, ranging from probing exotic forms of quantum matter to solving challenging real-world problems that can be naturally encoded on the qubits.

"This work enables a vast number of new scientific directions," Ebadi said. "We are nowhere near the limits of what can be done with these systems."

46.The Top 18 Research Institutions Leading the Recent Surge of Quantum Computing Investigations

by Matt Swayne
https://thequantumdaily.com/2021/07/07/the-top-18-research-institutions-leading-the-recent-surge-of-quantum-computing-investigations/

So far, 2021 has been a banner year for quantum computing. Several quantum-based companies have moved to go public, including at least two announcements of special acquisition companies being created to accommodate interest in quantum. Multinational corporate mergers have also started to happen in the quantum industry.

According to data gathered from Microsoft Academic, several universities and research institutions are consistently producing research papers, conference presentations and other forms of academic output in the quantum area. The groups represent both corporate research teams and university-based scientists.

Here are the top research institutions at this point in 2021, about midway through the year.

Number 1 — IBM

IBM was mentioned in about 786 pieces of research output so far this year.

IBM research teams and research equipment were involved in research output including the papers, Quantum Computer Systems for Scientific Discovery, Evidence of the entanglement constraint on wave-particle duality using the IBM Q quantum computer (Physical Review A) and Application of Quantum Machine Learning to High Energy Physics Analysis at LHC using IBM Quantum Computer Simulators and IBM Quantum Computer Hardware, presented at 2021 Proceedings of 40th International Conference on High Energy physics.

Find out more about IBM's quantum efforts here.

Number 2 — Massachusetts Institute of Technology

Massachusetts Institute of Technology — better known as MIT — is a world-renowned center for science, technology and engineering. MIT has been a pioneering hub for work in quantum. In 2021, researchers from MIT played roles in major advanced in quantum technology that were published in leading scientific journals, including: Room-temperature photonic logical qubits via second-order nonlinearities, which appeared in Nature Communications; Capturing Non-Markovian Dynamics on Near-Term Quantum Computers, Physical Review Research; and Creating Majorana modes from segmented Fermi surface, again in Nature Communications.

Find out more about quantum information science at MIT here.

Number 3 — Harvard University

Harvard continually makes lists for various scientific achievements. It is perennially on the top of lists for quantum science. According to Microsoft Academic, this legacy as a global leader in science and quantum research continues in 2021, with more than 1,800 entries in the quantum computer category on the research. Some of the studies, published both in major scientific journals and pre-print servers, such as ArXiv, that include Harvard researchers are: Quantum Computing at the Frontiers of Biological Sciences in Nature Methods; Quantum Information and Algorithms for Correlated Quantum Matter in Chemical Reviews and Quantum Computing and Quantum Information Storage in Physical Chemistry Chemical Physics.

Here's more information about Harvard's quantum initiative.

Number 4 — Max Planck Society

The Max Planck Society, established in 1948, has produced 20 Nobel laureates and is considered one of the world's most prestigious research institutions worldwide. Its scientists are producing cutting-edge research in the fields of quantum computing, as well. This year, MPS is among the leaders in quantum computing research. So far in 2021, Max Planck Society scientists have published "A Auantum-logic Gate Between Distant Quantum-network Modules" in Science and "Topological Two-Dimensional Floquet Lattice on a Single Superconducting Qubit" in Physical Review Letters, among dozens of other published research pieces.

Quantum science at the Max Planck Society is covered here.

Number 5 — University of Chicago

In the U.S. the heartland is also the heart of quantumland, thanks, in no small part, to the University of Chicago. In 2021, University of Chicago researchers have taken part in several key quantum computing studies including, "Engineering Dynamical Sweet Spots to Protect Qubits from 1 / f Noise," which appeared in Physical Review Applied; "Quantum Solver of Contracted Eigenvalue Equations for Scalable Molecular Simulations on Quantum Computing Devices," published in Physical Review Letters and "Orchestrated trios: compiling for efficient communication in Quantum programs with 3-Qubit gates," which was presented at ASPLOS 2021.

Chicago Quantum Exchange is a great resource for learning more about quantum science at the U of Chicago.

Number 6 — Chinese Academy of Sciences

The first Chinese entry on the list of top quantum research institutions is a research powerhouse in China. In just a few short months, the Chinese Academy of Sciences has amassed more than a thousand entries. Most recent entries in that list of quantum computing research advances are "Observation of energy-resolved many-body localization," published in Nature Physics; "A concise review of Rydberg atom based quantum computation and quantum simulation," Chinese Physics B and Solving quantum statistical mechanics with variational autoregressive networks and quantum circuits, which appeared in Machine Learning Science and Technology.

Read more about the academy's research advances here.

Number 7 — University of California, Berkeley

The University of California, Berkeley is located in the heart of California's quantum country. Its research output thus far this year — and its solid industrial and government connections — make it a top ten entrant on our list of

the most productive research institutions. Berkeley researchers contributed to published papers include: "Quantum approximate optimization of non-planar graph problems on a planar superconducting processor," in Nature Physics; "Efficient and noise resilient measurements for quantum chemistry on near-term quantum computers," npj Quantum Information and "Materials challenges for trapped-ion quantum computers," Nature Reviews Materials.

Read more about the University of California's quantum advances at Berkeley Quantum.

Number 8 — University of Maryland, College Park

Home of one of the first quantum computer firms to go public (IonQ) and a constant addition to TQD's "best of" lists, the University of Maryland, College Park is showing no signs of slowing down research output in the quantum computing field. UoM research teams participated in the following studies and published papers: "Probing many-body localization on a noisy quantum computer," Physical Review A; "Microwave Superconductivity," IEEE and "Conformal field theories are magical," Physical Review B.

Learn more about the Joint Center of Quantum Information and Computer Science.

Number 9 — Princeton University

The second Ivy League school in the list of top quantum research institutions is probably a no-brainer, if that term can be used without irony. Princeton has a well-established reputation as being one of the world's centers of academic and research excellence. That reputation continues in quantum. This year, Princeton researchers have participated in several quantum advances reported in journals and on pre-print servers, including "New material platform for superconducting transmon qubits with coherence times exceeding 0.3 milliseconds," Nature Communications; "Spin Digitizer for High-Fidelity Readout of a Cavity-Coupled Silicon Triple Quantum Dot," Physical Review Applied and "CutQC: using small Quantum computers for large Quantum circuit evaluations," ASPLOS 2021.

Learn more about quantum at Princeton here.

Number 10 — Google

From the company that developed the first quantum computer to assert quantum supremacy, Google researchers continue to make impressive strides in the quantum computing field. For this year, the company's scientists have taken part in studies, including "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," in Quantum; "High-Fidelity Measurement of a Superconducting Qubit Using an On-Chip Microwave Photon Counter," in Physical Review X and "Power of data in quantum machine learning," in Nature Communications.

Explore the possibilities of quantum with Google.

Number 11 — University of Tokyo

Japan is a hub of research into technology and information science. This research prowess extends to the quantum era. The University of Tokyo is home to scientists who took part in the following recent studies and published papers: "Blueprint for a scalable photonic fault-tolerant quantum computer," which appeared in Quantum; "Post-Hartree–Fock method in quantum chemistry for quantum computer," published in European Physical Journal and "Event Classification with Quantum Machine Learning in High-Energy Physics," presented in Computing and Software for Big Science.

Read more about this quantum initiative at the University of Tokyo.

Number 12 — University of Science and Technology of China

Our second entry to the list from China continues to astound the world with its scientific advances in quantum computing. Scientists from the University of Science and Technology of China have been involved in quantum computer studies, including: "Testing a Quantum Error-Correcting Code on Various Platforms," in Chinese Science Bulletin; "Experimental exploration of five-qubit quantum error correcting code with superconducting qubits," in National Science Review and "Quantum walks on a programmable two-dimensional 62-qubit superconducting processor" in Science.

Here's the Division of Quantum Physics and Quantum Information at USTC.

Number 13 — University of Washington

The Seattle-based University of Washington is growing into its role as one of the leaders in quantum science and, in particular, in quantum computing. A recent surge in published research papers about quantum computing include University of Washington researchers leading the charge. Those projects include: "Sparse-Hamiltonian approach to the time-evolution of molecules on quantum computers,"The European Physical Journal," "Entanglement rearrangement in self-consistent nuclear structure calculations," Physical Review C and "Qubit Regularization of Asymptotic Freedom" in Physical Review Letters.

You can read about one U of W quantum initiative here.

Number 14 — University of Oxford

The University of Oxford's contributions to quantum science are legendary. The university is now one of the leaders sherparding the world from classical to Noisy Intermediate Scale Quantum — NISQ — and beyond. Here are a few projects Oxford scientists are involved in that have implications in quantum computing: "Multi-exponential error extrapolation and combining error mitigation techniques for NISQ applications," which appeared in npj Quantum Information; Non-Gaussianity as a Signature of a Quantum Theory of Gravity, which was published in PRX Quantum and The prospects of quantum computing in computational molecular biology, which appeared in WIREs Computational Molecular Biology.

Here's an example of a quantum computer project at the University of Oxford.

Number 15 — Duke University

Duke University is probably not a research institution that most immediately associate with quantum computing compared to some of the other institutions. (Duke's research trail only leads back to 1998, while some of the other universities have quantum computing work that originated in the 1980s, even the 1970s…) But that's changing as the following quantum projects show: "Materials challenges for trapped-ion quantum computers," Nature Reviews Materials; "Optimizing Stabilizer Parities for Improved Logical Qubit Memories," ArXiv and "Practical Applications with Quantum Computers," presented at Quantum West.

As an example of Duke's forward-looking quantum progress, check out this initiative.

Number 16 — National Institute of Standards and Technology

The National Institute of Standards and Technology supports quantum science both in the U.S. and around the world. The soul of NIST's support is in the prowess of its researchers. Here are a few NIST-backed research projects: "Ray-Based Framework for State Identification in Quantum Dot Devices," PRX Quantum; "Towards data-driven next-generation transmission electron microscopy," Nature Materials and "Control and readout of a superconducting qubit using a photonic link," in Nature.

Read more about NIST's support of quantum in this TQD article.

Number 17 — Stanford University

Seated geographically right in the hottest of technological hot spots, Stanford University is among the top research institutions for the high tech world. In quantum computing, its recent publications show scientists involved in the following projects: "Quantum Permutation Synchronization," in ArXiv; "Recycling qubits in near-term quantum computers," in Physical Review A and "Connecting and scaling semiconductor quantum systems," presented at Photonic and Phononic Properties of Engineered Nanostructures XI

Read about Stanford's Quantum Computing mission here.

Number 18 — California Institute of Technology

You can't have Caltech without the tech part and it's rapidly becoming a quantum powerhouse. Just some of the work done recently by scientists at California Institute of Technology include: Power of data in quantum machine learning, in Nature Communications; "Low rank representations for quantum simulation of electronic structure," in npj Quantum Information and "Quantum Computation of Finite-Temperature Static and Dynamical Properties of Spin Systems Using Quantum Imaginary Time Evolution," in PRX Quantum.

CalTech quantum projects include the Institute for Quantum Information and Matter.

A Note on How This List Was Created

The above list is not meant to be exhaustive. Microsoft Academic was used to pull a list of the top research institutions publishing or presenting research on quantum computing, so far in 2021. Obviously, it is just a snapshot in time. The list could change because of publication schedules, timing of conferences, search terms, etc. and could include other limitations.

47.Quantum random number cloud platform

by npj quantum information
https://www.nature.com/articles/s41534-021-00442-x

Abstract: Randomness lays the foundation for information security. Quantum random number generation based on various quantum principles has been proposed to provide true randomness in the last two decades. The authors integrate four different types of quantum random number generators on the Alibaba Cloud servers to enhance cybersecurity. Post-processing modules are integrated into the quantum platform to extract true random numbers. They employ improved authentication protocols where original pseudo-random numbers are replaced with quantum ones. Users from the Alibaba Cloud, such as Ant Financial and Smart Access Gateway, request random numbers from the quantum platform for various cryptographic tasks. For cloud services demanding the highest security, such as Alipay

at Ant Financial, we combine the random numbers from four quantum devices by XOR the outputs to enhance practical security. The quantum platform has been continuously run for more than a year.

48.OQC Delivers the UK's first Quantum Computing as-a-Service

by Matt Swayne
https://thequantumdaily.com/2021/07/07/oqc-delivers-the-uks-first-quantum-computing-as-a-service/

Oxford Quantum Circuits (OQC) announced that the company has launched the nation's first commercially available Quantum Computing-as-a-Service built entirely using its proprietary technology.

In a boost for the UK's ambitions to be a global quantum superpower, as well as for businesses looking to explore the increasing commercial and technical benefits of quantum computing, today's announcement is the latest in a series of firsts for the company.

Having built and launched the UK's first superconducting quantum computer in 2018, today's announcement marks the first time OQC's proprietary technology is available to the enterprise via its private cloud. This announcement supports the startup's goal of pioneering the Quantum Computing-as-a-Service (QCaaS) market.

"The launch of our QCaaS platform is not only a remarkable achievement in the history of Oxford Quantum Circuits, but is a significant milestone in unlocking the potential of quantum computing both in the UK and globally," said Dr. Ilana Wisby, the CEO of OQC. "We know quantum computing has the power to be revolutionary but for decades this power and potential has been relatively untested and unverified in the real world. By making our QCaaS platform more widely available to strategic partners and customers, we are offering the world's leading enterprises the chance to demonstrate just how far-reaching quantum will be for their companies and their industries."

OQC's QCaaS is Now Accessible to Partners

OQC's Quantum Computing-as-a-Service platform takes its proprietary quantum technology to the market through a private cloud, where it will be used by strategic partners and customers to further experiment with quantum until ultimately they make breakthrough discoveries and tackle some of the world's most intractable problems.

OQC's partner, Cambridge Quantum, will be the first to be given access to the private cloud to demonstrate its IronBridge cybersecurity platform, which extracts perfect certified entropy from quantum computers to generate unhackable cryptographic keys. To achieve this milestone — of national strategic importance — Cambridge Quantum will have access to one of OQC's systems, "Sophia", hosted at the company's state-of-the-art lab in the UK. The facility, which was built last year amid the global pandemic, is the first commercial quantum computing laboratory in the country.

Following OQC's convention of naming its systems after women in STEM, this system is named after Sophia Jex-Blake: a British physician who led the campaign to secure women's access to a University education when she and six other women, collectively known as the 'Edinburgh Seven', began illegally studying medicine at the University of Edinburgh in 1869.

OQC is now welcoming registrations to its beta list, for sector-leading enterprise customers looking to take advantage of the technical and commercial benefits of quantum computing.

Scalability at a Fraction of the Cost

The launch of the OQC's Quantum Computing-as-a-Service platform is testament to the scalability of its patented architecture and technological designs. Leading quantum circuits to date have been built in a two-dimensional plane. In 2D, the intricate wiring required to control and measure the qubits — the core input-output functionality of the quantum hardware — quickly becomes a limiting factor as it introduces noise. Noise harms the coherence of the quantum device, which reduces the quality of its output. As the number of qubits grows, the intricacy of the wiring demands more fabrication steps, increasing error rates and cost.

OQC's core innovation, the Coaxmon, solves these challenges using a three-dimensional architecture that moves the control and measurement wiring out of plane and into a 3D configuration. This vastly simplifies fabrication, improving coherence and – crucially – boosting scalability.

This key advantage underpins the company's confidence in its strategy to "build the core and partner with the best". Just four years after it was founded, having attracted nearly £2m of UK government support and some of the leading scientists and engineers in the field, the pre-Series A startup is now a leader in the "noisy intermediate-scale quantum" (NISQ) era of quantum computing. Yet OQC is doing so with a fundamental advantage when it comes to scaling up to future generations of quantum machines. This radical design innovation and its proven effectiveness so far is driving the company in its mission to help its customers explore the possibilities of quantum advantage.

It is also a great example of the value of the National Quantum Technologies Programme in supporting excellent research and the growth of start-ups helping to create a vibrant UK quantum sector.

Bringing Quantum to the Enterprise

Businesses invited to join OQC's beta list will be able to test OQC's systems in streamlining or enhancing their business processes, and model and experiment with new approaches.

In the long-term, quantum could have a significant impact on businesses' operations, and on our lives:

- Pharmaceutical companies being able to look for ways to better predict health conditions, and identify new molecules
- Financial institutions getting great insight into their trading and risk management strategies
- Multinationals experimenting with quantum-enabled fleet logistics to optimise their supply chains and manufacturing
- The advancement of more efficient and powerful energy capture and storage for the future of battery technology
- The development of more powerful AI algorithms
- Cryptography and national security, and much more

Ilyas Khan, CEO of Cambridge Quantum said, "We are excited to be working with OQC on their first commercially available product. It has long been recognised that the first "killer app" for quantum computers will be in the area of cybersecurity, and we are looking forward to demonstrating that OQC can generate verifiably quantum cryptographic keys for our IronBridge platform." Khan added, "Ilana and her team represent the very best of breed in the hard-

ware sector in the UK and this bold launch of a quantum processor by a company that has very much been in stealth is a reminder of the depth and diversity of the UK's quantum technologies sector."

Digital Infrastructure Minister Matt Warman said, "The UK boasts some of the world's top innovators and research institutions and this partnership helps reinforce our position as a global leader in quantum computing. Quantum computing can help tackle some of the world's greatest challenges such as climate change, and UK firms can use this cutting-edge service to boost growth and innovation, and build back better from the pandemic."

49.Untappable quantum cryptography becomes practical with MDI-QKD

by Joshua Slater
https://qutech.nl/2021/07/06/untappable-quantum-cryptography-becomes-practical-with-mdi-qkd/

Engineers from QuTech can provide untappable communication that is cost-scaling to many users by using measurement-device independent (MDI) quantum key distribution (QKD). A notable side-feature is that, courtesy of Cisco, conventional internet operates in parallel, on the same optical fibre from Dutch telecom provider KPN. MDI-QKD is an important step towards an accessible quantum internet.

Presently secure communication is based on the fact that breaking cryptography is slow using conventional computers. This includes communication between datacentres, inter-governmental communication, or critical infrastructure like banking, energy and airports. Some communication lines require secrecy by law or by the user. Any attacker could be recording these messages and then decrypting them later. Unfortunately, computers are becoming faster, even more so with the impending introduction of quantum computers.

Ultimate defence against eavesdropping

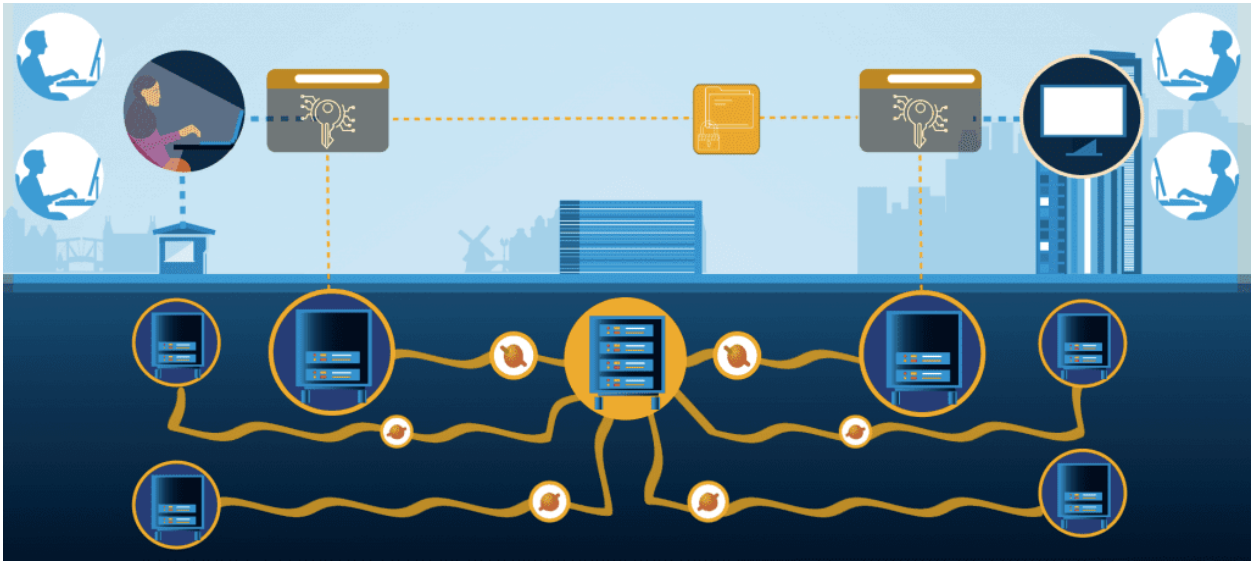
Joshua Slater, team lead of the MDI-QKD project: "Important conventional cryptographic methods rely on, for example, a public and a private key. These two keys are essentially two large numbers that belong together. Their security is based on the fact that the private key is difficult and slow to calculate with knowledge of only the public key. Unfortunately, with the introduction of very powerful computers (such as quantum computers), calculating the private key becomes trivially easy and then encryption can become insecure"

A solution to eavesdropping—now and in the future—is the use of quantum key distribution (QKD). In quantum communication, eavesdropping on a message disturbs transmission of the quantum key. Slater: "If the quantum signals are disturbed, the users know not to use the generated key for their secure communication line. Once the quantum key is successfully shared with the intended recipient, the rest of the secure communication benefits from 'forward secrecy': the assurance that the key distribution cannot be cracked now or in the future."

"Unfortunately, current commercially available QKD systems are difficult to scale in a network," Slater explained. "To solve all these problems, we've built a measurement-device independent (MDI) QKD system, in which multiple users can be connected via a central node that operates like a typical telephone switch board operator. Importantly, the central node does not need to be trusted. The entire system is designed such that hacking attacks against the central node cannot break the security of the protocol."

Scalable quantum networks

Slater: “A major advantage of our system over other QKD systems is its scaling to many users. Our MDI-QKD can be used in a star-type physical network. Researchers at QuTech have already previously performed the first proof-of-principle demonstration of MDI-QKD, the first demonstration over deployed fibres, and the first demonstration using cost-effective, off-the-shelf hardware.”



Because of the measurement-device independent (MDI) system the whole network is rather easy to scale up to many users.

“A significant achievement that we’re demonstrating here for the first time, is that our quantum signals are transmitted over the same fibre as conventional internet traffic,” said Slater. “Using standard equipment that Cisco supplied and configured with us, we established two multiplexed internet networks between the locations over the same optical fibres. The existence of these two networks do not impact the performance of our quantum system. Essentially, we’ve shown how our systems can coexist, in parallel”

“This is an important development in guaranteeing the security of internet traffic in the future,” said Babak Fouladi, Chief Digital and Technology Officer and member of the Executive Board at KPN. “I am pleased that we can contribute towards making this insight practical using the network of the Netherlands. Solutions like MDI-QKD should not only protect users today, but also make communication as future-proof as possible.”

Demonstration in Delft–Rijswijk–The Hague

The current system consists of three standard telco racks, each in a different city in the Netherlands. The first ‘user’ connected to the demo setup is code-named Alice and resides in Delft. The second user, called Bob, sits in a KPN building in The Hague. The central node, Charlie, is located in between. Every user is connected to the centre node by a standard optical fibre. Furthermore, the users and the central node are able to communicate over the normal internet, either directly via the (same) optical fibre, or indirectly via any internet connection.

Finally, the MDI-QKD deployment represents an important step towards a future quantum internet. The network is designed to be upgradable in the future: users like Alice and Bob can upgrade their functionality (with e.g. quantum processors, quantum repeaters, quantum entanglement, quantum memory, quantum computers, whatever), while the central node and the rest of the network remains the same. The network is future-proof and ready to be upgraded for the quantum future.

"This is a great milestone, and an important foundation for the deployment of a national quantum network infrastructure in the Netherlands. That is one of the main goals of the Netherlands' National Agenda Quantum Technology, which is being executed by Quantum Delta NL," said Jesse Robbers, director of Quantum Delta NL—which received €615 million from the Dutch government in April of this year.

50.China takes quantum supremacy lead

by Tibi Puiu
https://www.zmescience.com/science/china-takes-quantum-supremacy-lead/

Researchers in China have demonstrated the most powerful quantum computer in the world, **a 56-qubit machine** that can perform operations orders of magnitude faster than Google's quantum computer — its closest competitor. The Chinese quantum computer completed a complex calculation in a little over an hour, a task that would take a classical supercomputer eight years to perform.

China's quantum supremacy

The task performed by the new Zuchongzhi quantum computer is yet another demonstration of "quantum supremacy". The mythical-sounding term describes crossing the threshold where quantum computers can do things that conventional computers cannot in a reasonable timeframe.

Quantum computers exploit the mathematical quirks of the quantum world to vastly outperform classical computers.

Digital computers require data to be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), whereas quantum computers use qubits, also known as quantum bits, that can exist in multiple states simultaneously.

In 2019, Google's 54-qubit quantum processor, known as Sycamore, was the first in the world to achieve quantum supremacy. But its fame was soon overshadowed by Jiuzhang, an optical circuit 53-qubit quantum processor developed by researchers at the University of Science and Technology of China in Hefei.

Rather than superconducting materials on a chip, Jiuzhang uses optical circuits that perform calculations using photons instead of a flow of electrons as used by Google's Sycamore. Jiuzhang performed a complex task in 200 seconds that would have taken the fastest Chinese supercomputer, TaihuLight, around 2.5 billion years to arrive at the same result.

However, Jiuzhang is a one-trick pony. It's a specialized device that can't be programmed to perform any other task. So in many ways, Google's machine was much more practical despite the fact that Jiuzhang was much faster at completing its specialized task.

Now, researchers in China have demonstrated a much more versatile 66-qubit quantum computer, known as Zuchongzhi. The machine was developed by a team led by Jian-Wei Pan at the University of Science and Technolo-

gy of China in Shanghai and has 11 rows and 6 columns of qubits forming a two-dimensional rectangular lattice pattern.

Zuchongzhi used 56 of its qubits to complete a random quantum circuit sampling task, which the researchers call an "outstanding candidate to demonstrate quantum computational advantages." The idea is that this task is far too complex for a classical computer to solve in a reasonable timeframe and around 100 times more challenging than the one solved by Sycamore — but Zuchongzhi was up for it.

Zuchongzhi finished the sampling in 1.2 hours with just 56 qubits. This shows that the two-qubit edge over Sycamore matters a lot. Every additional qubit makes the quantum processor exponentially more powerful, which is why all of these advances are such a big deal.

> "We estimate that the classical computational overhead to simulate Zuchongzhi is 2-3 orders of magnitude higher than the task implemented on Google's 53-qubit Sycamore processor. Therefore, our experiment unambiguously established a computational task that can be completed by a quantum computer in 1.2 hours but will take at least an unreasonable time for any supercomputers," the Chinese researchers wrote in the pre-print server *ArXiv*.

51.Quantum-Safe Encryption Product Ready To Scale

by James Dargan
https://thequantumdaily.com/2021/07/05/quantum-safe-encryption-product-ready-to-scale/

NISQ Era

There is not a shred of doubt that quantum computers—when they reach their full potential—will have exponentially more computational power than the most powerful supercomputers on the planet. Fundamentally different in every way possible, most of them on offer now by the likes of IBM and Google are early versions of what experts in the field call Noisy Intermediate-Scale Quantum (NISQ) Computers. These have high error rates with each operation they perform, and though they're not world-changing at the moment, we are starting to see how they could be used to great effect for applications in quantum chemistry and quantum simulations.
In cybersecurity, too, we are witnessing advances in Post-Quantum Cryptography (PQC) and Quantum Random Number Generation (QRNG). Though it is early days, the threat of quantum computing is a near and present danger and we have to be prepared.

01 Communique

In view of this, the large corporations of industry, smaller companies and nimble startups are trying to come up with valuable solutions in Quantum-Safe Cryptography. One such company is 01 Communique and its IronCAP™ range of Post-Quantum products.

Founded way back in 1992, 01 Communique is a Toronto-based company loaded with innovations and accomplishments. Its latest technological breakthrough is in cybersecurity, and especially Quantum-Safe solutions utilizing its patent-pending IronCAP™ cryptography.

Its IronCAP™ API can be used by vendors to build highly secure systems for data storage, credit card security, remote access, encryption, digital signing, etc., which can protect their customers from cyberattacks not only today but also in the quantum future. 01 has used the IronCAP™ API to build the world's first end-to-end email/file encryption and digital signing system called IronCAP X™. It can be easily integrated into your current email system such as Outlook, Gmail, Yahoo etc., and help to safeguard against phishing emails. Both products are designed to operate on conventional computer systems to nullify future attacks from quantum computers.

When *TQD* asked Andrew Cheung—01 Communique Laboratory Inc's president and CEO—about the product, his response was enlightening:

> *"We believe IronCAP'™s quantum-safe encryption solution is the best-in-class cryptography solution. It has stood the test of time—passing the due diligence of its big-name partners and has successfully completed two global hackathons unscathed."*

He also commented there is increasing concern about privacy and the protection of personal information, as well as realizing it is important to understand the impact of big cybersecurity threats and what can be done to keep enterprises and individuals secure.

Too Early or Too Late

While this is clear enough, Cheung added that making the switch in encryption methods will be a little bit of a chore but with new developments in quantum computing fast progressing every day, the question is whether people have the foresight to deploy quantum-resistant encryption may be two years too early, or risk installing it two years too late.

All insightful information, no doubt, as it compounds the fact Cheung and his team are on the front foot as far as the inflection point goes within the industry, noticeable apparent in the CEO's remark about the Bitcoin ATM machine and crypto E-wallet protected by IronCAP™. According to Cheung, "*Once hailed as unhackable, the blockchains are now under close scrutiny, especially for their endpoint infrastructure. We welcome ixFintech's leading industry foresight to adopt the IronCAP™ technology to protect valuable digital assets—not only today—but also in the fast-approaching quantum era.*"

By complying with the PKCIS#11 and OpenPGP (RFC4880) industry standards, the IronCAP API allows all kinds of vertical applications such as password management, credit card security, cloud storage, and website security—along with those already mentioned—to be transformed into quantum-safe. 01 Communique's IronCAP™ solution is one to watch out for.

52.French researchers on the verge of quantum computing milestone

by Dhananjay Khadilkar
https://www.rfi.fr/en/science-and-technology/20210705-french-researchers-on-the-verge-of-quantum-computing-milestone

Researchers at the French Alternative Energies and Atomic Energy Commission (CEA) in Grenoble are confident of reaching a key milestone at the end of this year in their quest to build a quantum computer.

Maud Vinet and Silvano De Franceschi from the CEA along with Tristan Meunier of CNRS are leading a multidisciplinary team of around 50 scientists and engineers to build a silicon based quantum machine, the first critical step of which would be to operate a network of two qubits in the coming months.

How quantum computing works

Qubits are the units of information in quantum computing. They are the quantum equivalent of bits. Unlike classical computing where bits can exist as either 0 or 1, in quantum systems they possess both values at the same time. This property is called superposition.

The other key quantum property is called entanglement. It refers to the almost instantaneous effect two qubits have on each other even at a distance after having been initially coupled. Entanglement and superposition give quantum computers their phenomenal calculating power.

But keeping qubits entangled is a big challenge. “It is subject to interference from the environment. Any disturbances, whether thermal, electrical or mechanical, can cause errors,” De Franceschi says.

One way to limit the errors caused by these factors is to operate the qubits in a deep freeze mode.

“When qubits are cooled down to sufficiently low temperature, typically below a few degrees Kelvin, they are no longer susceptible to undesirable thermal excitations and their coherence can be preserved,” Vinet says.

Though the system to cool qubits uses the similar principle as that of a household refrigerator, it is much bigger and way more complex.

The CEA has several cryostats that use helium to achieve a temperature between 15 millikelvin to 1 Kelvin.

That corresponds to 272 degrees below water’s freezing point. Besides the above-mentioned cryostats, the CEA also boasts of a cryogenic prober that can carry out automatic measurements of 300 mm silicon wafers below 2 Kelvin or minus 271 degree Celsius. There are only two such machines in the world.

The French approach

There are four major approaches to fabricate the qubits: **photons**, **trapped ions**, **superconductors** and **semiconductors like silicon**.

Vinet and De Franceschi have adopted the last approach which involves the use of the magnetic moment of an electron in silicon to create the two different states of the qubit. They have chosen silicon even though it seems to be lagging behind the others in terms of the number of interacting qubits in a network.

“The other three approaches seem to have made more progress. But we are sticking with silicon. That’s because building workable quantum computers is not a short term race. It doesn’t matter where you stand today. What matters more is the growth potential for the future,” De Franceschi told RFI.

According to Vinet, in order to build a practical quantum computer, scalability will be the key. “In this regard, there’s no better candidate than silicon, which is central to the semiconductor industry. With silicon we can fabricate

millions or even billions of qubits that can be assembled in a relatively compact system. It's also convenient for control electronics."

Moreover, according to De Franceschi, when it comes to performance, the silicon qubits are on par with the other platforms in terms of fidelity and speed of operations. De Franceschi contends that some of the other approaches may be appropriate but they may not be equally suitable when it comes to effective, massive and easy manufacturing.

"You need to consider how good you can scale up and handle the controlling of qubits once the processor size grows. There are other problems such as possible interference when you are manipulating qubits. The successful approach will be the one that copes the best with all these issues," he says.

Researchers at CEA have a unique advantage as both the physics and the engineering requirements necessary to build a quantum computer are available under the same roof.

While De Franceschi and his team are engaged in perfecting the fabrication and interactions between qubits, Vinet and his group are working in parallel to make qubits truly scalable and to build the other components of a quantum computer.

"What we are trying to do here is build a full stack quantum computer. We are developing the quantum chip, control electronics, implementation of the quantum algorithm as well as an interface that translates the algorithm into electrical signals," Vinet says.

Quantum appeal

Quantum computers have elicited huge interest from not just research labs but also IT giants, start ups and governments. In January 2021, French President Emmanuel Macron announced a 1.8 billion euro Quantum Plan initiative for supporting research and development of quantum technologies.

The enormous appeal of quantum computing lies in its promise to easily outperform even the world's most powerful supercomputers on certain types of calculations.

"They are expected to solve complex problems such as protein simulations, calculating air flow on aircraft, finding new materials such as possibly room temperature superconductors," Vinet says, adding researchers still don't know how powerful these machines will turn out to be.

53.Ransomware hits hundreds of US companies, security firm says

by AP
https://indianexpress.com/article/technology/tech-news-technology/ransomware-hits-hundreds-of-us-companies-security-firm-says-7387089/lite/

A ransomware attack paralyzed the networks of at least 200 U.S. companies on Friday, according to a cybersecurity researcher whose company was responding to the incident.

The **REvil gang**, a major Russian-speaking ransomware syndicate, appears to be behind the attack, said John Hammond of the security firm Huntress Labs. He said the criminals targeted a software supplier called Kaseya, using its network-management package as a conduit to spread the ransomware through cloud-service providers. Other researchers agreed with Hammond's assessment.

"Kaseya handles large enterprise all the way to small businesses globally, so ultimately, (this) has the potential to spread to any size or scale business," Hammond said in a direct message on Twitter. "This is a colossal and devastating supply chain attack."

Such cyberattacks typically infiltrate widely used software and spread malware as it updates automatically.

It was not immediately clear how many Kaseya customers might be affected or who they might be. Kaseya urged customers in a statement on its website to immediately shut down servers running the affected software. It said the attack was limited to a "small number" of its customers.

Brett Callow, a ransomware expert at the cybersecurity firm Emsisoft, said he was unaware of any previous ransomware supply-chain attack on this scale. There have been others, but they were fairly minor, he said.

"This is SolarWinds with ransomware," he said. He was referring to a Russian cyberespionage hacking campaign discovered in December that spread by infecting network management software to infiltrate U.S. federal agencies and scores of corporations.

Cybersecurity researcher Jake Williams, president of Rendition Infosec, said he was already working with six companies hit by the ransomware. It's no accident that this happened before the Fourth of July weekend, when IT staffing is generally thin, he added.

"There's zero doubt in my mind that the timing here was intentional," he said.

Hammond of Huntress said he was aware of four managed-services providers — companies that host IT infrastructure for multiple customers — being hit by the ransomware, which encrypts networks until the victims pay off attackers. He said thousand of computers were hit.

"We currently have three Huntress partners who are impacted with roughly 200 businesses that have been encrypted," Hammond said.

Hammond wrote on Twitter: "Based on everything we are seeing right now, we strongly believe this (is) **REvil/Sodinikibi**." The FBI linked the same ransomware provider to a May attack on JBS SA, a major global meat processer.

The federal Cybersecurity and Infrastructure Security Agency said in a statement late Friday that it is closely monitoring the situation and working with the FBI to collect more information about its impact.

CISA urged anyone who might be affected to "follow Kaseya's guidance to shut down VSA servers immediately." Kaseya runs what's called a virtual system administrator, or VSA, that's used to remotely manage and monitor a customer's network.

The privately held Kaseya says it is based in Dublin, Ireland, with a U.S. headquarters in Miami. The Miami Herald recently described it as "one of Miami's oldest tech companies" in a report about its plans to hire as many as 500 workers by 2022 to staff a recently acquired cybersecurity platform.

Brian Honan, an Irish cybersecurity consultant, said by email Friday that "this is a classic supply chain attack where the criminals have compromised a trusted supplier of companies and have abused that trust to attack their customers."

He said it can be difficult for smaller businesses to defend against this type of attack because they "rely on the security of their suppliers and the software those suppliers are using."

The only good news, said Williams, of Rendition Infosec, is that "a lot of our customers don't have Kaseya on every machine in their network," making it harder for attackers to move across an organization's computer systems.

That makes for an easier recovery, he said.

Active since April 2019, the group known as **REvil provides ransomware-as-a-service**, meaning it develops the network-paralyzing software and leases it to so-called affiliates who infect targets and earn the lion's share of ransoms.

REvil is among ransomware gangs that steal data from targets before activating the ransomware, strengthening their extortion efforts. The average ransom payment to the group was about half a million dollars last year, said the Palo Alto Networks cybersecurity firm in a recent report.

Some cybersecurity experts predicted that it might be hard for the gang to handle the ransom negotiations, given the large number of victims — though the long US holiday weekend might give it more time to start working through the list.

54.Government to unveil national cyber security strategy soon: National Cyber Security Coordinator

by PTI
https://www.thehindu.com/business/government-to-unveil-national-cyber-security-strategy-soon-national-cyber-security-coordinator/article35119538.ece

National Cyber Security Coordinator Rajesh Pant said the strategy would holistically cover the entire ecosystem of cyber space in India.

The government will release a new cybersecurity strategy this year, National Cyber Security Coordinator Rajesh Pant said at an event organised by Public Affairs Forum of India (PAFI).

He said the strategy would holistically cover the entire ecosystem of cyber space in India.

The government is expected to release a new cybersecurity strategy this year, he said speaking at the PAFI event on Friday.

"The vision of this strategy is to ensure safe, secure, resilient, vibrant, and trusted cyber space," Mr. Pant said.

The new strategy would serve as a guideline to tackle various aspects, be it data as a national resource, building indigenous capabilities or cyber audit.

“There are about 80 odd deliverables coming out of this new strategy,” the PAFI statement quoted Mr. Pant as saying.

The theme of the PAFI Dialogue was ‘**Cyber Security in the New Normal**.’ On the national security narrative for the telecom sector, Mr. Pant said, “While other nations have created a black-list of companies that cannot operate in the country, India is the only nation to create a white-list of telecom companies that are allowed to operate in India”

The companies allowed must be a ‘trusted source’, he said adding, “We were able to create and launch the trusted telecom portal during the pandemic and within six months.”

55.Russia using Kubernetes cluster for brute-force attacks

by Shaun Nichols

https://searchsecurity.techtarget.com/news/252503482/Russia-using-Kubernetes-cluster-for-brute-force-attacks?utm_campaign=20210707_NSA+sounds+alarm+on+Russian+container-based+attacks%3B+Plus%2C+REvil+ransomware+returns&utm_medium=EM&utm_source=NLN&track=NL-1820&ad=939572&asrc=EM_NLN_169456182

The NSA is sounding the alarm over a fresh wave of Kremlin-backed attacks on both the U.S. government and private sector companies.

The intelligence agency issued an alert Thursday over what it describes as brute-force password attacks that are being launched from a specially-crafted Kubernetes cluster. The attacks have been attributed to a unit within Russia's foreign intelligence agency, the General Staff Main Intelligence Directorate (GRU); the NSA said it's the same GRU unit that has been identified as the APT28 or Fancy Bear threat group, which has been responsible for several attacks on U.S. targets, such as the 2016 breach of the Democratic National Committee.

In this case, the NSA warned, European companies are also in the crosshairs. In addition to government agencies, the GRU hackers have been going after media companies, defense contractors, think tanks and political groups, and energy providers, among other industries.

“This campaign has already targeted hundreds of U.S. and foreign organizations worldwide, including U.S. government and Department of Defense entities,” the NSA said in the alert. “While the sum of the targeting is global in nature, the capability has predominantly focused on entities in the U.S. and Europe.”

The NSA declined to comment on what the success rate of the attacks has been, and just how many networks have actually been compromised by the hackers.

The brute-force attacks are part of a larger effort to harvest credentials and gain a foothold in networks. After the automated brute-force operation nets valid user accounts, the attackers shift to a more hands-on approach.

The stolen accounts are used to log into the targeted company's network, where the attackers then look to exploit elevation of privilege and remote code execution vulnerabilities to obtain administrator rights; these vulnerabilities

include two Microsoft Exchange Server flaws, CVE 2020-0688 and CVE 2020-17144. From there, the hackers look to move laterally through the network, eventually arriving at a mail server or other valuable data cache.

Once the data and account details have been collected and uploaded to another server, the attackers install web shells and administrator accounts, giving them persistence on the network and the ability to get back in at a later date.
While the NSA says that most of the attacks were launched from behind the cover of Tor and multiple VPN services, the attackers did get sloppy on occasion, and some of the attacks went directly from the Kubernetes cluster, allowing investigators to collect a handful of IP addresses.

56.Quantum Computing just got desktop sized

by Adrian Pennington

https://www.redsharknews.com/quantum-computing-just-got-desktop-sized

Quantum computing is coming on leaps and bounds. Now there's an operating system available on a chip thanks to a Cambridge University-led consortia with a vision is make quantum computers as transparent and well known as RaspberryPi.

This "sensational breakthrough" is likened by the Cambridge Independent Press to the moment during the 1960s when computers shrunk from being room-sized to being sat on top of a desk.

Around 50 quantum computers have been built to date, and they all use different software – there is no quantum equivalent of Windows, IOS or Linux. The new project will deliver an OS that allows the same quantum software to run on different types of quantum computing hardware.

The system, Deltaflow.OS (full name Deltaflow-on-ARTIQ) has been designed by Cambridge Uni startup Riverlane. It runs on a chip developed by consortium member SEEQC using a fraction of the space necessary in previous hardware. SEEQC is headquartered in the US with a major R&D site in the UK.

"In its most simple terms, we have put something that once filled a room onto a chip the size of a coin, and it works," said Dr. Matthew Hutchings, chief product officer and co-founder of SEEQC in a press statement.

"This is as significant for the future of quantum computers as the microchip itself was for commercialising traditional computers, allowing them to be produced cost-effectively and at scale."

Quantum computers store information in the form of quantum bits, or qubits. Like Schrödinger's cat (which would not have had the colloquial impact had he chosen an inanimate object), qubits can exist in two different information states at the same time.

But for quantum computers to be truly powerful they must be able to scale up to include many more qubits, making it possible to solve some seriously challenging problems

"Where it took a rackful of electronics to control the qubits, now it's available on a chip the size of a penny," Hutchings explained. "All the functionality is on a chip, so we've solved the issue for the quantum era."

57.Computing Breakthrough: Unveiling Properties Of New Superconductor

by Disha Sinha
https://www.analyticsinsight.net/quantum-computing-breakthrough-unveiling-properties-of-new-superconductor/

The collaboration of the School of Physics and Astronomy, of the University of Minnesota and Cornell University, has revealed some unique properties of a new semiconductor such as a superconducting metal. It has created a breakthrough in quantum computing and can be utilized in the nearby future. The metal is known as Niobium diselenide (NbSe2) that can conduct electricity or transport electrons or photons without any resistance. Quantum computing can reap the benefits of this new superconducting metal effectively and efficiently for new innovations.

Niobium diselenide is in 2D form with two-fold symmetry that makes it a more resilient superconductor. There are two types of superconductivity found in this metal— conventional wave-type consisting of bulk NbSe2 and unconventional d- or p- wave type for a few layers of NbSe2. These both have the same kind of energies due to the constant interaction and competition between each other. The research teams from both universities have combined the results of two different experimental techniques to generate this ground-breaking discovery. The scientists wanted to investigate the properties of NbSe2 further to able to use unconventional superconducting states to develop advanced quantum computers.

Superconducting metals, help to explore the boundaries between quantum computing and traditional computing with applications in quantum information. The quantum bits transform the functionalities of quantum computers with much higher speed than the traditional ones. Quantum bits exist in a superposition state along with two values 0 and 1 simultaneously with alpha and beta. Quantum computers require around 10,000 qubits to work smartly and help in the entanglement of nature's mysteries. Superconductors can create a solid state of the qubit with quantum dots and single-donor systems. These superconductor metals are known for transforming electrons into a single superfluid that can move through a metal lattice without any resistance.

The discovery of 2D crystalline superconductors has opened a plethora of methods to investigate unconventional quantum mechanics. The top-notch quality of monolayer superconductor, NbSe2, is grown by chemical vapor deposition. The growth of these superconductors depends on the ultrahigh vacuum or dangling bond-free substrates that help to reduce environment and substrate-induced defects.

Hence, the world is waiting for further discoveries of some unique properties of any superconducting metal to help in the advancement of quantum computing that can bring certain breakthroughs in industries.

58.Understanding potential topological quantum bits

by Institute of Science and Technology Austria
https://www.sciencedaily.com/releases/2021/07/210701140937.htm

The Quantum computers promise great advances in many fields -- from cryptography to the simulation of protein folding. Yet, which physical system works best to build the underlying quantum bits is still an open question. Unlike

regular bits in your computer, these so-called qubits cannot only take the values 0 and 1, but also mixtures of the two. While this potentially makes them very useful, they also become very unstable.

One approach to solve this problem bets on topological qubits that encode the information in their spatial arrangement. That could provide a more stable and error-resistant basis for computation than other setups. The problem is that no one has ever definitely found a topological qubit yet.

An international team of researchers from Austria, Copenhagen, and Madrid around Marco Valentini from the Nano-electronics group at IST Austria now have examined a setup which was predicted to produce the so-called Majorana zero modes -- the core ingredient for a topological qubit. They found that a valid signal for such modes can in fact be a false flag.

Half of an Electron

Entanglement The experimental setup is composed of a tiny wire just some hundred nanometers -- some millionths of a millimeter -- long, grown by Peter Krogstrup from Microsoft Quantum and University of Copenhagen. These appropriately-called nano-wires form a free-floating connection between two metal conductors on a chip. They are coated with a superconducting material that loses all electrical resistance at very low temperatures. The coating goes all the way up to a tiny part left at one end of the wire, which forms a crucial part of the setup: the junction. The whole contraption is then exposed to a magnetic field.

The scientists' theories predicted that Majorana zero modes -- the basis for the topological qubit they were looking for -- should appear in the nanowire. These Majorana zero modes are a strange phenomenon, because they started out as a mathematical trick to describe one electron in the wire as composed of two halves. Usually, physicists do not think of electrons as something that can be split, but using this nanowire setup it should have been possible so separate these “half-electrons” and to use them as qubits.

"We were excited to work on this very promising material platform," explains Marco Valentini, who joined IST Austria as an intern before becoming a PhD student in the Nano-electronics group. "What we expected to see was the signal of Majorana zero modes in the nanowire, but we found nothing. First, we were confused, then frustrated. Eventually, and in close collaboration with our colleagues from the Theory of Quantum Materials and Solid State Quantum Technologies group in Madrid, we examined the setup, and found out what was wrong with it."

A False Flag

TheAfter attempting to find the signatures of the Majorana zero modes, the researchers began to vary the nanowire setup to check whether any effects from its architecture were disturbing their experiment. "We did several experiments on different setups to find out what was going wrong," Valentini explains. "It took us a while, but when we doubled the length of the uncoated junction from a hundred nanometers to two hundred, we found our culprit.”

When the junction was big enough the following happened: The exposed inner nanowire formed a so-called quantum dot -- a tiny speck of matter that shows special quantum mechanical properties due to its confined geometry. The electrons in this quantum dot could then interact with the ones in the coating superconductor next to it, and by that mimic the signal of the “half-electrons” -- the Majorana zero modes -- which the scientists were looking for.

“This unexpected conclusion came after we established the theoretical model of how the quantum dot interacts with the superconductor in a magnetic field and compared the experimental data with detailed simulations performed by Fernando Peñaranda, a PhD student in the Madrid team,” says Valentini.

“Mistaking this mimicking signal for a Majorana zero mode shows us how careful we have to be in our experiments and in our conclusions,” Valentini cautions. “While this may seem like a step back in the search for Majorana zero modes, it actually is a crucial step forward in understanding nanowires and their experimental signals. This finding shows that the cycle of discovery and critical examination among international peers is central to the advancement of scientific knowledge.”