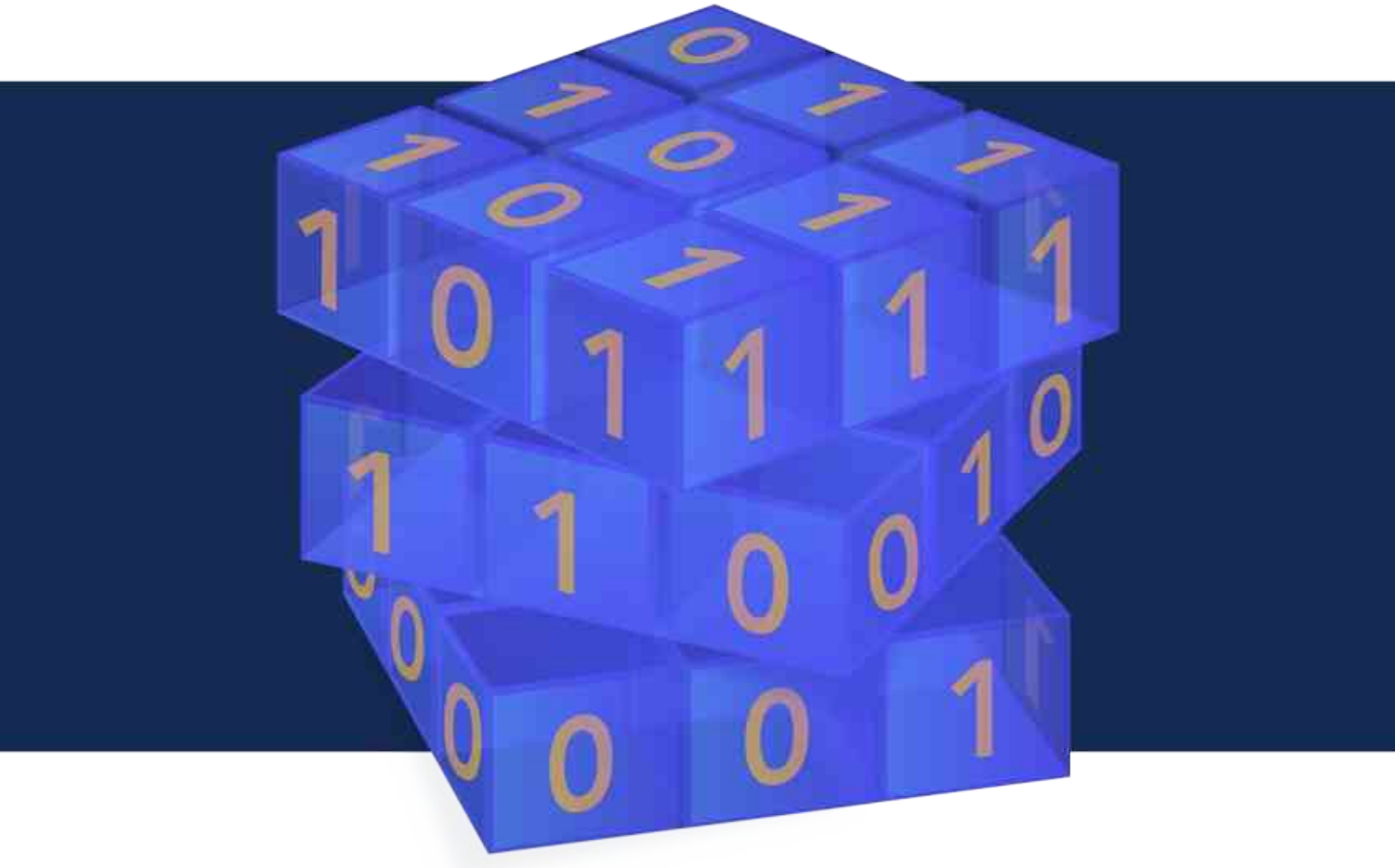
Crypto News

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

October 01, 2021



1. Editorial

SEATTLE, WA – October, 1st, 2021. Ready for another one? The October issue of Crypto News is here! This month's newsletter **includes several articles about cryptography** and how to prepare organizations for quantum computing so be sure to check those out. In addition to those, there are some other great articles as well.

Take a look **at Article 3 which focuses on Majorana zero (MZM)** quasiparticles and some recent setbacks. Though current findings are throwing the topological quantum computing field into crisis mode, it should be noted that industry professionals still have faith in its future use for quantum computing. Something to keep an eye on! Next, let's **talk about ethics**. The recent focus on quantum computing ethics is important and should be pursued. However, there are suggestions to start by addressing classical computing ethics and grow from there. Check out **article 27** for more details on how to get started. **Article 51** makes an interesting and timely observation about silos of information in regards to cyberattacks in U.S. agencies. The article points to similar missteps made prior to the U.S. 9/11 attacks. Is it already too late? Keep reading to find out more! You won't want to miss the other articles either!

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

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

2. Russian Scientists Use Supercomputer to Probe Limits of Google's Quantum Processor

by SKOLTECH
https://scitechdaily.com/russian-scientists-use-supercomputer-to-probe-limits-of-googles-quantum-processor/

CPQM's Laboratory for Quantum Information Processing has collaborated with the CDISE supercomputing team "Zhores" to emulate Google's quantum processor. Reproducing noiseless data following the same statistics as Google's recent experiments, the team was able to point to a subtle effect lurking in Google's data. This effect, called a reachability deficit, was discovered by the Skoltech team in its **past work**. The numerics confirmed that Google's data was on the edge of a so-called, density-dependent avalanche, which implies that future experiments will require significantly more quantum resources to perform quantum approximate optimization. The results are published in the field's leading journal *Quantum*.

From the early days of numerical computing, quantum systems have appeared exceedingly difficult to emulate, though the precise reasons for this remain a subject of active research. Still, this apparently inherent difficulty of a classical computer to emulate a quantum system prompted several researchers to flip the narrative.

Scientists such as Richard Feynman and Yuri Manin speculated in the early 1980s that the unknown ingredients which seem to make quantum computers hard to emulate using a classical computer could themselves be used as a computational resource. For example, a quantum processor should be good at simulating quantum systems, since they are governed by the same underlying principles.

Such early ideas eventually led to Google and other tech giants creating prototype versions of the long-anticipated quantum processors. These modern devices are error-prone, they can only execute the simplest of quantum programs and each calculation must be repeated multiple times to average out the errors in order to eventually form an approximation.

Among the most studied applications of these contemporary quantum processors is the quantum approximate optimization algorithm, or QAOA (pronounced "kyoo-ay-oh-AY"). In a series of dramatic experiments, Google used its processor to probe QAOA's performance using 23 qubits and three tunable program steps.

In a nutshell, QAOA is an approach wherein one aims to approximately solve optimization problems on a hybrid setup consisting of a classical computer and a quantum co-processor. Prototypical quantum processors such as Google's Sycamore are currently restricticted to performing noisy and limited operations. Using a hybrid setup, the hope is to alleviate some of these systematic limitations and still recover quantum behavior to take advantage of, making approaches such as QAOA particularly attractive.

Skoltech scientists have made a series of recent discoveries related to QAOA, for example see the write-up **here**. Prominent among them being an effect that fundamentally limits the applicability of QAOA. They show that the density of an optimization problem — that is, the ratio between its constraints and variables — acts as a major barrier to achieving approximate solutions. Additional resources, in terms of operations run on the quantum co-processor, are required to overcome this performance limitation. These discoveries were done using pen and paper and very small emulations. They wanted to see if the effect they recently discovered manifested itself in Google's recent experimental study.

Skoltech's quantum algorithms lab then approached the CDISE supercomputing team led by Oleg Panarin for the significant computing resources required to emulate Google's quantum chip. Quantum laboratory member, Senior Research Scientist Dr. Igor Zacharov worked with several others to transform the existing emulation software into a form that permits parallel computation on Zhores. After several months, the team managed to create an emulation that outputs data with the same statistical distributions as Google and showed a range of instance densities at which QAOA performance sharply degrades. They further revealed Google's data to lie at the edge of this range beyond which the current state of the art would not suffice to produce any advantage.

The Skoltech team originally found that reachability deficits — a performance limitation induced by a problem's constraint-to-variable ratio — were present for a kind of problem called maximum constraint satisfiability. Google, however, considered the minimization of graph energy functions. Since these problems are in the same complexity class, it gave the team conceptual hope that the problems, and later the effect, could be related. This intuition turned out to be correct. The data was generated and the findings clearly showed that reachability deficits create a type of an avalanche effect, placing Google's data on the edge of this rapid transition beyond which longer, more powerful QAOA circuits become a necessity.

Oleg Panarin, a manager of data and information services at Skoltech, commented: "We are very pleased to see our computer pushed to this extreme. The project was long and challenging and we've worked hand in glove with the quantum lab to develop this framework. We believe this project sets a baseline for future demonstrations of this type using Zhores."

Igor Zacharov, a senior research scientist at Skoltech, added: "We took existing code from Akshay Vishwanatahan, the first author of this study, and turned it into a program that ran in parallel. It was certainly an exciting moment for all of us when the data finally appeared, and we had the same statistics as Google. In this project, we created a software package that can now emulate various state-of-the-art quantum processors, with as many as 36 qubits and a dozen layers deep."

Akshay Vishwanatahan, a PhD student at Skoltech, concluded: "Going past a few qubits and layers in QAOA was a significantly challenging task at the time. The in-house emulation software we developed could only address toy-model cases and I initially felt that this project, while an exciting challenge, would prove nearly impossible. Fortunately, I was amidst a group of optimistic and high-spirited peers and this further motivated me to follow through and reproduce Google's noiseless data. It was certainly a moment of great excitement when our data matched Google's, with a similar statistical distribution, from which we were finally able to see the effect's presence."

3. Major Quantum Computing Strategy Suffers Serious Setbacks

by Philip Ball
https://www.quantamagazine.org/major-quantum-computing-strategy-suffers-serious-setbacks-20210929/

In 2018, researchers at the forefront of an entirely new approach to building quantum computers published, in the journal *Nature*, what looked to be a landmark achievement. Existing quantum computers are notoriously fragile, their quantum bits — qubits — prone to incurring random errors. But if the qubits could be made from strange configurations of electrons with the exotic name of Majorana zero-mode (MZM) quasiparticles, errors simply couldn't occur. An MZM qubit can no more suffer a random error than you can separate the links of a chain without cutting them — the basic principles of topology, the mathematics of shape, protects against it.

These "topological" qubits are extremely difficult to build, but despite the technical challenges, some researchers are convinced that they are the only path to building a useful quantum computer with many hundreds or thousands of qubits. Microsoft, for one, is staking its main quantum computing strategy on topological qubits.

That's one reason why the 2018 *Nature* paper garnered so much attention. A team led by Leo Kouwenhoven, a physicist at the Delft University of Technology in the Netherlands, said that they had found the definitive signature of MZM quasiparticles in indium antimonide nanowires. Their paper was heralded, with much press fanfare, as the dawn of topological quantum computing. In 2019, Microsoft opened its own quantum laboratory on the Delft campus, with Kouwenhoven as its director.

Then things started to fall apart. Later that year, Sergey Frolov, a physicist at the University of Pittsburgh, and his collaborator Vincent Mourik of the University of New South Wales in Australia were doing similar work in their own labs. (Both Frolov and Mourik are former members of Kouwenhoven's group.) Frolov and Mourik found they couldn't reproduce the Delft results. That October the duo asked Kouwenhoven's group for their raw data, and in December they found some odd inconsistencies: It looked as though some of the plots had been manipulated, and the paper's claims weren't borne out when the full range of measurements was taken into account.

Faced with these problems, Kouwenhoven's group replotted their data and found the conclusions no longer stood up. In March 2021, at Kouwenhoven's request, *Nature* retracted the paper. The group wrote in their retraction that they could "no longer claim the observation of a quantized Majorana conductance." They added an apology "for insufficient scientific rigour in our original manuscript."

The incident triggered an investigation by an independent committee. The investigation concluded that there was no evidence of fraudulent data fabrication or manipulation. The authors had simply fooled themselves by zooming in only on the results that showed them what they hoped to see. "The research program the authors set out on is particularly vulnerable to self-deception, and the authors did not guard against this," the authors of the report wrote.

"It was an unfortunate incident of overzealousness combined with being careless," said Patrick Lee, a physicist at the Massachusetts Institute of Technology and a member of the committee.

The retraction, along with other recent high-profile examples of related work that fell apart under closer inspection, has exposed an additional challenge at the heart of topological quantum computing research: Not only is it extremely difficult to build a topological qubit, but no one is sure how to even spot one. The quantum rules that lead to MZM quasiparticles also allow the creation of other weird quantum states — states that mimic Majorana particles but can't be used as the basis for a quantum computer.

Because of these and other hurdles, the field of topological quantum computing has entered a period of self-reflection, if not outright crisis. "I've become concerned that, after a series of false starts, a significant fraction of the Majorana field is fooling itself," Frolov wrote in a commentary in *Nature* in April. Yet despite this problem, even the field's critics find the science too promising to ignore. "The physics behind the creation of Majoranas is well understood theoretically," said Frolov in an interview. "Usually when that happens in condensed matter physics, the physical realization is not far behind. I am quite confident that within the next couple years, one or more groups will find strong evidence for them."

.
.
.

4. Photonic chip is key to 'nurturing' quantum computers

by University of Bristol
https://www.sciencedaily.com/releases/2021/09/210929101843.htm

A team of researchers from Bristol's Quantum Engineering and Technology Labs (QETLabs) has shown how to protect qubits from errors using photons in a silicon chip.

Quantum computers are gaining pace. They promise to provide exponentially more computing power for certain very tricky problems. They do this by exploiting the peculiar behaviour of quantum particles, such as photons of light.

However, quantum states of particles are very fragile. The quantum bits, or qubits, that underpin quantum computing pick up errors very easily and are damaged by the environment of the everyday world. Fortunately, we know in principle how to correct for these errors.

Quantum error correcting codes are a method to protect, or to nurture, qubits, by embedding them in a more robust entangled state of many particles. Now a team led by researchers at Bristol's Quantum Engineering and Technology Laboratories (QETLabs) has demonstrated this using a quantum photonic chip.

The team showed how large states of entangled photons can contain individual logical qubits and protect them from the harmful effects of the classical world. The Bristol-led team included researchers from DTU in Copenhagen who fabricated the chip.

Dr Caterina Vigliar, first author on the work, said: "The chip is really versatile. It can be programmed to deliver different kinds of entangled states called graphs. Each graph protects logical quantum bits of information from different environmental effects."

Anthony Laing, co-Director of QETLabs, and an author on the work said: "Finding ways to efficiently deliver large numbers of error protected qubits is key to one day delivering quantum computers."

5. Far Fewer Qubits Required for "Quantum Memory" Quantum Computers

by Erika K. Carlson
https://physics.aps.org/articles/v14/s117

So far, research on quantum memory—units for storing quantum information—has largely focused on its use in quantum communications and networks. Now, Élie Gouzien and Nicolas Sangouard of the French Alternative Energies and Atomic Energy Commission have investigated how quantum memory might be used in computations. The duo shows that a quantum computer architecture that incorporates a quantum memory could perform calculations with 3 orders of magnitude fewer qubits in its processor than standard architectures require, making the devices potentially easier to realize.

Researchers consider superconducting qubits one of the most promising technologies for building a quantum computer. But a challenge of using such qubits is that a large number are required for the standard superconducting-qubit-computer architecture, whose processor typically consists of a 2D grid of qubits in which computations are done using interactions of neighboring qubits.

In their work, Gouzien and Sangouard instead considered a 2D grid of qubits connected to a quantum memory that is organized in 3D. To compare this architecture to the standard one, they analyzed how it should perform the task of finding the prime factors for very large integers called RSA integers. They found that this quantum computer design with a quantum memory could factor a 2048-bit RSA integer with just 13,436 qubits, while the standard architecture, with no quantum memory, might require some **twenty million qubits** for this task.

The standard architecture is estimated to take just 8 hours for the factorization, whereas the quantum memory architecture would require 177 days. But Gouzien and Sangouard say that the approach is worth further investigation, as the substantially smaller number of qubits required makes the approach much more feasible in the near-term.

6. IBM CEO: Quantum computing will take off 'like a rocket ship 'this decade

by MARK SULLIVAN
https://www.fastcompany.com/90680174/ibm-ceo-quantum-computing-will-take-off-like-a-rocket-ship-this-decade

IBM is one of the best-known names in technology, and yet most people would struggle to explain exactly what the company does. That's understandable. The Armonk, New York-based tech mainstay has often reinvented itself, and is in the process of becoming a hybrid cloud company that serves artificial intelligence services—a core business resembling Amazon's AWS or Microsoft's Azure.

"Going from tabulating machines to electronic calculators to the first semiconductor-based computers to today's day of hybrid cloud and AI . . . that is a remarkable series of revolutions, not just evolutions," IBM chairman and CEO Arvind Krishna told *Fast Company* technology editor Harry McCracken during an interview recorded for the Fast Company Innovation Festival.

At a practical level IBM makes its money selling business software and middleware, hosting the data and content of enterprises, helping enterprises manage data that lives on their own servers, and providing a range of services related to everything from healthcare AI to nanotechnology.

Krishna boiled down IBM's work as an effort to help businesses and organizations apply technology to their processes and systems. He gave examples, noting that IBM helped the Social Security Administration figure out people's incomes so that it knew what to pay beneficiaries. It also helped a credit card company authorize payments without fraud, and it "helps the federal reserve move trillions of dollars through the economy each day," he said.

Fast Company named IBM to its Most Innovative Companies list in 2020 for the company's on-location incubators, which are helping small startups and organizations transform their business via tech, such as a wireless company that was able to turn older cars into voice-enabled smart cars.

IBM is already preparing for its next reinvention. Quantum computing spent a long time in the realm of the theoretical. Now it's in the realm of research labs, including IBM's. And soon—very soon, if you ask Krishna—it will escape the lab and begin making a real difference in the business world. IBM, of course, wants to be front and center when that happens.

IBM finished its first quantum system, the IBM Q System One, in 2019. The System One is a 20-qubit system, meaning that it operates on 20 quantum bits. These qubits are the basic units of computing, comparable to the atomic-size bits used in regular computers. Bits, however, can exist only in two states—one or zero. Qubits are subatomic and move far faster than bits; quantum computers must operate in extremely cold temperatures so that the quantum state of the materials inside can be controlled. And most important, qubits can occupy two physical states at once. They can be zero and one at the same time. This is known as "superposition" in quantum physics, and it opens up new vistas of opportunity for scientists trying to model complex problems.

Superposition is why quantum computers may eventually be useful in solving problems that concern levels of risk, such as in logistics, supply chain management, or resource optimization.

"All of these problems are probabilistic in nature," Krishna said. "A digital computer works at hard zeros and ones—you're not trying to impose probability on it. Quantum computing is probabilistic by nature; it lives in that maybe/maybe-not state. And so those problems map naturally onto a quantum computer."

1,000 QUBITS AND BEYOND

Krishna believes that quantum computers, including IBM's, will begin growing in size toward 1,000-qubit systems. "We put out a road map saying a thousand cubits by the end of 2023," Krishna said. As the number of qubits grows, these supercomputers will begin being used to solve real business problems—such as managing agricultural risk—in the latter half of this decade.

"And once it starts, it's going to take off like a rocket ship . . .," Krishna told McCracken. "Because let's suppose one capital markets institution uses it to get a better price arbitrage on some financial instrument, don't you think everybody else will want to do it then, instantly?"

The larger the systems, the broader the applications and addressable problems. Krishna noted that the technical barriers that must be overcome to get from 20- to 1,000-qubit systems exist in the realm of "engineering" problems. But getting from a thousand to a million qubits is a different matter.

"As we scale towards a million, I think we've got some fundamental issues in error correction, control, and maybe quantum physics that can rear their heads," he said, adding that even those problems are "solvable."

IBM remains one of the most prolific research organizations in the world. It recently designed the first semiconductor based on a 2 nanometer manufacturing process, which will soon be produced by Samsung and others. It's likely that IBM will play a big role in the push toward big quantum computers that have the power to solve some of the world's biggest problems.

7. Quantum computing hits the desktop, no cryo-cooling required

by Loz Blain
https://newatlas.com/quantum-computing/quantum-computing-desktop-room-temperature/

An Australian/German company is developing powerful quantum accelerators the size of graphics cards. They work at room temperature, undercutting and outperforming today's huge, cryo-cooled quantum supercomputers, and soon they'll be small enough for mobile devices.

Superconducting quantum computers are huge and incredibly finicky machines at this point. They need to be isolated from anything that might knock an electron's spin off and ruin a calculation. That includes mechanical isolation, in extreme vacuum chambers, where only a few molecules might remain in a cubic meter or two of space. It includes electromagnetic forces – IBM, for example, surrounds its precious quantum bits, or qubits, with mu metals to absorb all magnetic fields.

And it includes temperature. Any atom with a temperature above absolute zero is by definition in a state of vibration, and any temperature more than 10-15 thousandths of a degree above absolute zero simply shakes the qubits to the point where they can't maintain "coherence." So most state-of-the-art quantum computers need to be cryogenically cooled using complex and expensive equipment before the qubits will maintain their state for any length of time and become useful.

Extreme vacuums, mu metals and microkelvin-temperature cryogenic cooling: this is not a recipe for affordable, portable or easily scalable quantum computing power. But an Australian-born startup says it has developed a quantum microprocessor that needs none of these things. Indeed, it runs happily at room temperature. Right now, it's the size of a rack unit. Soon, it'll be the size of a decent graphics card, and before too long it'll be small enough to fit in mobile devices alongside traditional processors.

If this company does what it says it can, you'll be able to integrate the advantages of quantum into computers of just about any size, freeing this powerful new technology from the constraints of supercomputer size and expense. Quantum software and calculations won't need to be done through a fast connection to a mainframe or the cloud, it'll be done on-site where it's needed. Pretty disruptive stuff.

Quantum Brilliance was founded in 2019 on the back of research undertaken by its founders at the Australian National University, where they developed techniques to manufacture, scale and control qubits embedded in synthetic diamond.

This is complex business, so we'll throw over to the Quantum Brilliance whitepaper for a technical description: "Room-temperature diamond quantum computers consist of an array of processor nodes. Each processor node is comprised of a nitrogen-vacancy (NV) center (a defect in the diamond lattice consisting of a substitutional nitrogen atom adjacent to a vacancy) and a cluster of nuclear spins: the intrinsic nitrogen nuclear spin and up to ~4 nearby 13C nuclear spin impurities. The nuclear spins act as the qubits of the computer, whilst the NV centers act as quantum buses that mediate the initialization and readout of the qubits, and intra-and inter-node multi-qubit operations. Quantum computation is controlled via radiofrequency, microwave, optical and magnetic fields."

This field itself is not new – indeed, room-temperature quantum qubits have been around experimentally for more than 20 years. Quantum Brilliance's contribution to the field is in working out how to manufacture these tiny things precisely and replicably, as well as in miniaturizing and integrating the control structures you need to get information in and out of the qubits – the two key areas that have held these devices back from scaling beyond a few qubits to date.

"Because diamond is such a rigid material," says QB co-founder and COO Mark Luo over a Zoom call, "it's really able to hold a lot of these properties in place – that allow these quantum phenomena to be more stable compared to other systems out there. Given that rigidity, we can actually leverage off a lot of pre-existing classical control systems."

"The fundamental property we're using," says new hire Mark Mattingley-Scott, who will oversee operations for the company in Germany, "is nuclear spin, and not the spin of an electron. An atom cares a lot less about thermal vibrations, for example, than an electron, so this way we can run them at room temperature. In the nitrogen vacancy, there's a hole, and through that we're able to interact with the qubits. There are multiple interactions, so we actually get potentially multiple qubits per vacancy."

The company has already built a number of "Quantum development kits" in rack units, each with around 5 qubits to work with, and it's placing them with customers already, for benchmarking, integration, co-design opportunities and to let companies start working out where they'll be advantageous once they hit the market in a ~50-qubit "Quantum Accelerator" product form by around 2025. "We think over a decade," says Luo, "we can even produce a quantum system-on-a-chip for mobile devices. Because this is truly material science technology that can achieve that."

"In terms of commercial deployment," says Luo, "we have the Pawsey Supercomupting Center, which is currently the Southern Hemisphere's largest supercomputing center, co-owned by CSIRO and some other universities. We established basically Australia's first supercompuing quantum innovation hub, and we set up a Pawsey Pioneer program where industry and research groups can utilize our quantum operating system. We're deploying the world's first room-temperature diamond quantum computing system at Pawsey in Q1 2022 – we were meant to install it this month, but due to COVID delays we can't actually cross the borders into Western Australia! We're planning to deploy some in Germany as well, which is why we're so lucky to have Mark coming on board to lead our operations in Europe and Germany."

How do they perform compared to traditional superconducting quantum computers? Extremely well, says Mattingley-Scott. "There's a figure of merit which you can apply to the ability of individual qubits to be useful, and that's coherence time. Superconducting qubits typically hold their coherence for maybe 100, 150 microseconds. In room temperature diamonds, we're talking about milliseconds. Like, a thousand times longer, and that means you can do a lot more. That's part of the equation; the other part is error rates. Qubits, fundamentally, have an error rate, even before they lose coherence and descend into pure randomness. The error rates we get with nitrogen vacancy qubits are very, very good."

"So," he continues, "the basic answer is yes, these are very powerful qubits, and what you can do with these qubits is going to be more powerful than what you can do with superconducting qubits, because you have longer to work with them, and they hold their state."

So when will one of these things reach the storied milestone of quantum supremacy, becoming more powerful than any supercomputer at solving specific laboratory tests? In this case, that's not the focus. "We have a clear five-year roadmap to produce something we call quantum utility," says Luo. "Other systems can't miniaturize, we can miniaturize. So for us it's about producing a quantum computer or quantum accelerator that outperforms a classical computer of the same size, weight and power. It's outperforming the components within a supercomputer rather than outperforming entire supercomputers, in order to provide commercial utility."

The Quantum Brilliance vision is to make qubits an easily-integrated extra string to any computer's bow. Something like today's high-end graphics cards, produced in mass quantities to work in a broad range of systems at low unit costs. Software developers can then use traditional computing where that's advantageous and quantum only where it shines.

That could be in tasks that involve simulating pretty much anything with an atomic structure that exhibits quantum mechanical behavior; Mattingley-Scott lists pharmacological drug development, battery electrode development and energy generation as fields where this kind of gear could make an immediate impact. It could be in the linear algebra and matrix-style operations that underpin a lot of machine learning and AI – an explosively growing field in itself – and it could be highly useful in tasks that involve optimization, for example trying to reduce energy usage across the entire global business structure of a large logistics company.

"The potential business impact of quantum computing," says Mattingley-Scott, "is that it's going to fundamentally change almost everything we do, and the way we do it. I had a long, 32-year career at IBM, and for the last five of those I was running IBM's Ambassador Program, essentially a pre-sales and tech sales channel for quantum computing. And I had my eye on what was happening with diamonds, because if you can strike out the requirement to cryogenically cool your computer, it completely reframes the value proposition. So I've had Quantum Brilliance on my radar for some time, there's no other company working on a value proposition like this. And when the opportunity came along, that's why I joined."

"So with our five-year plan to get to that graphics card-sized Quantum Accelerator," he continues, "there's lots of uncertainties, and unknown variables. But we're not waiting for any magical new technology. There are no gaps. We know how to get to that device, we just have to roll up our sleeves and do it. And industrialize things, and get the yields and capacities up and that good stuff. But that's essentially the stuff the semiconductor industry has proven itself very good at, and we'll be leveraging that. So I can't give you exact dates, but that's where we're headed to, an industrialized type volume business."

8. EVERYTHING YOU MUST KNOW ABOUT UNHACKABLE QUANTUM INTERNET

by Madhurjya Chowdhury
https://www.analyticsinsight.net/everything-you-must-know-about-unhackable-quantum-internet/

Building quantum networks may sound like a science-fiction notion, yet it is a major goal for many governments across the world. For cryptography and optimization issues, quantum computers hold a lot of potentials. What quantum computers will and won't be able to achieve, as well as the obstacles we still face, are explored by ZDNet.

In this article, you will learn everything you must know about the unhackable quantum internet.

What is Quantum Internet?

The quantum internet is a network that will allow quantum devices to exchange data in an environment that uses quantum physics 'strange principles. In principle, this would provide the quantum internet unrivalled powers that are currently difficult to achieve with web apps.

Data may be encoded in the quantum realm using qubits, which are produced in quantum devices such as a quantum computer or a quantum CPU. In simple words, the quantum internet will include transmitting qubits over a network of many physically isolated quantum devices. All of this would be possible because of the bizarre characteristics that are specific to quantum states.

That sounds a lot like the ordinary internet. However, transmitting qubits over a quantum channel rather than a conventional one basically means exploiting the behaviour of particles at their tiniest size – so-called "quantum states" – which have long fascinated and perplexed physicists.

Why Quantum Internet?

QKD technology is still in its infancy. At the moment, the "standard" method of generating QKD is to deliver qubits one-way to the receiver through optical fibre cables; however, this severely limits the protocol's efficacy.

Because qubits may quickly get lost or dispersed in a fibre-optic cable, quantum signals are extremely error-prone and have a hard time travelling great distances. In reality, current tests are restricted to a few hundred kilometres in range.

Another option, which is the foundation of the quantum internet, is to use another quantum feature called entanglement to exchange messages devices.

When 2 qubits connect and entangle, they share qualities that are dependent on one another. Even though the qubits are physically removed, every change to one will lead to alterations to the other when they're in an entangled state.

The state of the first qubit may thus be "read" by observing its entangled counterpart's activity. In the setting of quantum communication, entanglement may effectively transfer some data from one qubit to its entangled opposite half, eliminating the need for a physical link to connect the two.

Quantum Information Exchange

In a nutshell, most consumers aren't used to much. You shouldn't anticipate being able to join quantum Zoom meetings any time soon, at least not in the next several decades. The fact that qubits, which employ quantum physics ' fundamental rules, behave substantially differently from classical bits is fundamental to quantum communication.

A classical bit can only have one of two states since it encodes data. A bit must be either 0 or 1, just like a light switch must be either on or off, and just like a cat must be either dead or living.

Qubits, on the other hand, are a different storey. Qubits, on the other hand, are superposed: they may be both 0 and 1 at the same time, in a quantum state that does not exist in the classical era. It's as if you might be on both the left side of your sofa at the same time.

The paradox is that just measuring qubit results in it being assigned a state. A measured qubit, like a traditional bit, falls out of its dual state and is demoted to 0 or 1. Superposition is the name for the whole phenomena, which is at the heart of quantum mechanics. Unfortunately, qubits can't convey the types of data we're used to, such as emails and Facebook messages.

Quantum Communications

Security is among the most intriguing topics that researchers using qubits are pursuing.

When it comes to traditional communications, most data is protected by giving the sender and recipient a shared key and then encrypting the message with that key. The recipient can then decrypt the data at their end using their key.

The security of most traditional communication today is built on a key generation process that is difficult, but not impossible, for hackers to crack. That is why scientists are attempting to make this communication mechanism "quantum." The notion lies at the heart of quantum key distribution, a new branch of cybersecurity.

Unhackable Quantum Internet

Quantum physics-based internets will soon enable fundamentally secure communication.

In recent years, scientists have discovered how to transport pairs of photons through fibre-optic cables in such a way that the information stored in them is completely protected. A Chinese team utilised a variant of the technique to build a 2,000-kilometre matching circuit connecting Beijing and Shanghai.

The technique is based on entanglement, a quantum property of atomic particles. It is impossible to interpret entangled photons without destroying their content. Entangled particles, on the other hand, are difficult to produce and even more difficult to transport across vast distances. Quantum repeaters that expand the network will be required to provide an uninterrupted connection across longer distances.

Conclusion

The objective for quantum researchers is to expand the networks up to a national level initially and then to a global one in the future. The great majority of experts agree that this will not happen in the next few decades. However, the quantum internet is a long-term endeavour with several technological hurdles to overcome. However, the unforeseen results that the technology will undoubtedly bring about along the road will make for an amazing scientific adventure, complete with a slew of bizarre quantum applications that can't even be predicted right now.

9. Dell Technologies test hybrid emulation platform for quantum computing via Qiskit

by Larry Dignan
https://www.zdnet.com/article/dell-technologies-test-hybrid-emulation-platform-for-quantum-computing-via-qiskit/

Dell Technologies said it has been testing a hybrid emulation platform that can enable developers to run quantum applications on classical infrastructure.

In a blog post, Dell Technologies CTO John Roese outlined the emulation platform, which used Dell EMC PowerEdge R740xd and IBM's Qiskit Runtime, an open-source container service for quantum computers.

With technology teams exploring quantum computing for operations in the future, Roese said simulators and emulators will be needed. Dell Technologies is betting that the quantum computer won't replace all classical computing. Both quantum and classical compute will be accessed via the cloud most likely, he added.

For developers, the win is being able to use the Dell-IBM emulation platform to test applications, algorithms and other use cases. Details of the Dell Technologies' hybrid emulation platform are posted on Github.

Key points include:

- The hybrid emulation platform executes on both classical and quantum processing on cloud native platforms like Kubernetes. Previously, developers had to submit data and workloads for processing via the cloud.
- Each quantum circuit no longer needs to be executed and wait in queue separately.
- Workloads can be run on-premises.
- The hybrid approach may save money by giving developers choices to optimize for costs.

10. Valleytronics for quantum computing at room temperature

https://www.thehindubusinessline.com/business-tech/valleytronics-for-quantum-computing-at-room-temperature/article36683323.ece

IIT-Bombay team looks for a way to encode, process and store quantum information at less-restrictive temperatures

Quantum computers are hot today, because of their mind boggling computing capacity that can better the best of existing supercomputers. They use the quantum phenomenon of superposition. However, quantum phenomena do not work at room temperature. Existing quantum computers, such as those of Google, IBM, and Microsoft, have to be kept at ultra-low temperatures of –196.1°C , making them costly and impractical.

Researchers at IIT-Bombay have used an emerging science, called 'valleytronics', to pave the way for 'room temperature quantum computers'. Valleytronics is the study of location of electrons — the valleys refer to the local minima in the 'conduction 'energy bands (the range of energy an electron needs to fly away from the atom).

"Valleys can be used to encode, process and store quantum information at less-restrictive temperatures," notes an article presented by IIT-Bombay.

A team of its scientists, working in collaboration with the German Max-Born Institute, have used graphene for this. Prof Gopal Dixit, who led the research, says: "By tailoring the polarisation of two beams of light according to graphene's triangular lattice, we found it possible to break the symmetry between two neighbouring carbon atoms and exploit the electronic band structure in the regions close to the valleys, inducing valley polarisation." In other words, this enables the use of graphene's valleys to effectively "write" information. Conducting valley operations in graphene is possible at room temperature.

11. Top 10 Cybersecurity Threats

by Shelby Hiter
https://www.datamation.com/security/cybersecurity-threats/

The cybersecurity threats landscape is growing and increasing its negative impacts on companies, with cybercrime causing nearly $1 trillion in damage in 2020, according to "The Hidden Costs of Cybercrime" report by McAfee.

Cyber attacks grew during the earliest days of the COVID-19 pandemic, as employees began to work remotely and enterprises rushed their digital transformation efforts to meet the needs of a new working landscape.

Companies across the globe have learned several valuable lessons about securing their globally distributed infrastructure, both from witnessing large-scale data breaches and experiencing their own security incident scares.

As organizations continue to learn more about trending cybersecurity threats and the best ways to prevent them, it's important to remember: cybersecurity threats are the product of both external malicious actors and internal vulnerabilities.

Trending Cybersecurity Threats To Watch

(1) Ransomware and as-a-service attacks
(2) Enterprise security tool sprawl
(3) Misconfigured security applications at scale
(4) Sophisticated spear phishing strategies
(5) Increased frequency of credential theft
(6) Mobile device and OS vulnerabilities left unchecked
(7) Data governance and management errors
(8) Distributed growth of insider threats post-COVID
(9) Poorly secured cloud environments
(10) Incomplete post-attack investigations

12. Next Generation Reservoir Computing: A New Way to Solve the "Hardest of the Hard" Computer Problems

by OHIO STATE UNIVERSITY
https://scitechdaily.com/next-generation-reservoir-computing-a-new-way-to-solve-the-hardest-of-the-hard-computer-problems/

A relatively new type of computing that mimics the way the human brain works was already transforming how scientists could tackle some of the most difficult information processing problems.

Now, researchers have found a way to make what is called **reservoir computing** work between 33 and a million times faster, with significantly fewer computing resources and less data input needed.

In fact, in one test of this next-generation reservoir computing, researchers solved a complex computing problem in less than a second on a desktop computer.

Using the now current state-of-the-art technology, the same problem requires a supercomputer to solve and still takes much longer, said Daniel Gauthier, lead author of the study and professor of physics at The Ohio State University.

"We can perform very complex information processing tasks in a fraction of the time using much less computer resources compared to what reservoir computing can currently do," Gauthier said.

"And reservoir computing was already a significant improvement on what was previously possible."

The study was published on September 21, 2021, in the journal *Nature Communications*.

Reservoir computing is a machine learning algorithm developed in the early 2000s and used to solve the "hardest of the hard" computing problems, such as forecasting the evolution of dynamical systems that change over time, Gauthier said.

Dynamical systems, like the weather, are difficult to predict because just one small change in one condition can have massive effects down the line, he said.

One famous example is the "**butterfly effect**," in which – in one metaphorical example – changes created by a butterfly flapping its wings can eventually influence the weather weeks later.

Previous research has shown that reservoir computing is well-suited for learning dynamical systems and can provide accurate forecasts about how they will behave in the future, Gauthier said.

It does that through the use of an **artificial neural network**, somewhat like a human brain. Scientists feed data on a dynamical network into a "reservoir" of randomly connected artificial neurons in a network. The network produces useful output that the scientists can interpret and feed back into the network, building a more and more accurate forecast of how the system will evolve in the future.

The larger and more complex the system and the more accurate that the scientists want the forecast to be, the bigger the network of artificial neurons has to be and the more computing resources and time that are needed to complete the task.

One issue has been that the reservoir of artificial neurons is a "black box," Gauthier said, and scientists have not known exactly what goes on inside of it – they only know it worksThe artificial neural networks at the heart of reservoir computing are built on mathematics, Gauthier explained.

"We had mathematicians look at these networks and ask, 'To what extent are all these pieces in the machinery really needed?'" he said.

In this study, Gauthier and his colleagues investigated that question and found that the whole reservoir computing system could be greatly simplified, dramatically reducing the need for computing resources and saving significant time.

They tested their concept on a forecasting task involving a weather system developed by Edward Lorenz, whose work led to our understanding of the butterfly effect.

Their next-generation reservoir computing was a clear winner over today's state—of-the-art on this Lorenz forecasting task. In one relatively simple simulation done on a desktop computer, the new system was 33 to 163 times faster than the current model. But when the aim was for great accuracy in the forecast, the next-generation reservoir computing was about 1 million times faster. And the new-generation computing achieved the same accuracy with the equivalent of just 28 neurons, compared to the 4,000 needed by the current-generation model, Gauthier said.

An important reason for the speed-up is that the "brain" behind this next generation of reservoir computing needs a lot less warmup and training compared to the current generation to produce the same results.

Warmup is training data that needs to be added as input into the reservoir computer to prepare it for its actual task.

"For our next-generation reservoir computing, there is almost no warming time needed," Gauthier said."Currently, scientists have to put in 1,000 or 10,000 data points or more to warm it up. And that's all data that is lost, that is not needed for the actual work. We only have to put in one or two or three data points," he said.

And once researchers are ready to train the reservoir computer to make the forecast, again, a lot less data is needed in the next-generation system.

In their test of the Lorenz forecasting task, the researchers could get the same results using 400 data points as the current generation produced using 5,000 data points or more, depending on the accuracy desired.

"What's exciting is that this next generation of reservoir computing takes what was already very good and makes it significantly more efficient," Gauthier said.

He and his colleagues plan to extend this work to tackle even more difficult computing problems, such as forecasting fluid dynamics.

"That's an incredibly challenging problem to solve. We want to see if we can speed up the process of solving that problem using our simplified model of reservoir computing."

13. How Quantum Computing can Solve Real-World Problems

by LONNE JAFFE
https://devops.com/how-quantum-computing-can-solve-real-world-problems/

The history of technology can seem like it was very predictable in retrospect, but the future typically feels more uncertain. Nowhere is this uncertainty more evident than in the domain of quantum computing. When the spectrum of possible outcomes spans from "quantum computers will be one of the most important technology developments of all time" to "quantum computing may never really become practical enough to justify using over a classical computer alternative," trying to make forecasts can seem futile. However, as a technologist, investor, consumer or just a curious observer, the boundaries and texture of the uncertainty itself can be very interesting, valuable and informative.

Quantum computing isn't likely a replacement for today's classical computing—at least not initially—but rather a potential complement to it for specific applications. A 2021 report by Deloitte lists dozens of applications that could be transformed by quantum computing approaches: Protein folding, fluid simulation, credit underwriting, financial risk analysis, supply chain optimization and forecasting, vehicle routing, fraud detection, fault analysis, weather forecasting, semiconductor chip design, product-portfolio optimization, consumer product recommendations—and this is only half the list.

Quantum computing could make previously intractable simulation, search and optimization calculations relatively easy and quick. For some kinds of calculations, a quantum computer could be mind-bendingly faster than a powerful classical computer could ever be. While today's classical computers running machine learning systems can make incredibly accurate predictions, quantum-based systems can, in theory, far outstrip their speed at certain prediction-related tasks.

The blend of physics, math and computer science behind quantum computers is fascinating, but complex. Computer scientist Scott Aaronson, one of the best science communicators, wrote a recent essay for *Quanta* magazine called, "Why Is Quantum Computing So Hard To Explain?"

To oversimplify, quantum computers are built around "qubits," which are subatomic-scale components, often kept at incredibly cold temperatures (think: Absolute zero) to minimize interference from the rest of the universe. These components can be put into a quantum physics state called "superposition" that allows them to, in a sense, take on many potential values at once. Even though their value is uncertain, reliable calculations and transformations can be performed on these qubits while in a superposition before being reduced to a more classical state, effectively parallelizing computations. Qubits in a quantum computer can also be entangled with one another (a phenomenon that Einstein referred to as "spooky action at a distance"), harnessing them as a team to increase the variety of logical calculations that it's possible to compute. For certain types of math—for example, searching for an optimal outcome from myriad options—quantum algorithms can seem close to instantaneous when compared to those that run on classical computing hardware.

Quantum Computing Challenges

Publicly available quantum computing has been on the horizon for decades, yet there's still no reliable forecast for when products capable of widespread adoption will get released, exactly what form the systems will take or how broad and deep quantum computing's impact will be. There are many technical challenges when it comes to getting a broadly applicable quantum computer to be useful at scale. And quantum computers are racing against classical computers, which have also been improving very rapidly in power, versatility and ease-of-use.

One important bottleneck for quantum computers is that correctly reading the results of a quantum calculation is prone to a very high error rate—the delicate superposition state can deteriorate before the correct result is presented as an output.

Aaronson explains it:

> *The problem, in a word, is decoherence, which means unwanted interaction between a quantum computer and its environment — nearby electric fields, warm objects, and other things that can record information about the qubits … The only known solution to this problem is quantum error correction… But researchers are only now starting to make such error correction work in the real world. When you read about the latest experiment with 50 or 60 physical qubits, it's important to understand that the qubits aren't error-corrected. Until they are, we don't expect to be able to scale beyond a few hundred qubits.*

Some theorists even believe a practical quantum computer is impossible to build because of the inherently high amount of "noise in the system." Mathematician Gil Kalai predicts that doing error correction to reduce that noise to a usable level would, by basic computing theorems, restrict the computer's number-crunching capacity so low as to be not worth using.

Nevertheless, researchers continue to chisel away at the challenge of error correction and to pass key technical milestones. For example, in July, Google researchers published a paper in *Nature* explaining how they have found a promising error-reduction method that scales as more qubits are added to a system.

Hardware, Software and App Landscape

There are several different approaches to quantum hardware. Rigetti and Oxford Quantum Circuits use superconducting quantum circuits, a more widespread approach favored also by Google, Microsoft, and IBM. IonQ (which is planning to go public via a SPAC transaction) and Honeywell (which recently announced a combination of its quantum computing unit with UK-based Cambridge Quantum Computing) use trapped ions. D-Wave uses quantum annealing, ColdQuanta is using cold atoms and Xanadu is using photonics. Each approach has its pros and cons, and each hardware technology faces a fluid set of shifting bottlenecks in reaching affordable scale. Work at the materials layer continues to advance as well, for example, Raicol Crystals is growing quantum quasi-phase matching crystals that can be used in applications as varied as quantum computing, sensing, encryption and communications. And it's not certain that there won't be another approach that leapfrogs them in solving the challenges of error correction and price.

Other companies, such as Quantum Machines, Q-CTRL and Seeqc, are building control hardware that can operate in the space between classical and quantum hardware. Control systems can exist at temperatures warmer than absolute zero, but colder than room temperature. Some of these systems involve both software and hardware and can perform tasks like monitoring the quantum processor's performance, performing error correction or serving as an abstraction layer connecting classical and quantum hardware.

There are also companies creating quantum computing application layer software, like Zapata Computing, Riverlane or QC Ware. This can include application frameworks, components, algorithms or even turnkey quantum computing applications. Classiq has software for quantum circuit synthesis. There's also a lot of interesting fundamental research happening at the software intersection between quantum computing and artificial intelligence – e.g. Zapata published work recently using IonQ's ion trap quantum system to train a machine learning system to generate high-quality handwritten digits with low error rates.

One of the first theoretical uses for quantum computing, proposed in 1994 by mathematician Peter Shor, would be to crack the RSA encryption widely used today to protect data. The threat spawned research into post-quantum cryptography, with researchers proposing multiple new approaches to encryption that would need to replace today's algorithms to preserve the privacy of data. Companies such as ISARA (quantum-resistant encryption) and Quantum Xchange (an out-of-band, symmetric key delivery platform) emerged to help prepare governments and companies now for a world where quantum-based, encryption-cracking algorithms start to work on breaking today's encryption.

There are several widely used software development kits (SDKs) that let developers write software for a quantum computer without actually having one to run it on. In fact, a kind of format war has already broken out between quantum computing development environments.

One widely-used quantum SDK is IBM QISKit, an open-source Python-based development kit for prototyping software and devices on simulators or IBM Quantum Experience, a cloud-based quantum service. ExxonMobil, Goldman Sachs, Boeing, JP Morgan, Samsung and PayPal are just a few of IBM Quantum's marquee customers. Google Cirq, another Python-based development kit, touts Volkswagen as a user, and Volkswagen is also a contributor to Google's TensorFlow Quantum, an open source library that extends Google's TensorFlow machine learning algorithms to quantum processors for rapid prototyping. Microsoft's Quantum Development Kit (QDK) is based on Microsoft's Q# programming language and brings quantum compatibility to Microsoft Azure cloud services. Early customers of Azure Quantum include Dow for chemical simulations and Toyota Tsusho, Toyota's trading arm, developing traffic light optimizations to reduce urban traffic congestion.

In a recent piece, The Information noted that "Amazon is looking to hire more than 100 new quantum computing scientists, hardware developers and engineers within its Amazon Web Services cloud business," following the enor-

mous amount of funding flowing to startups in the space, such as Quantum Motion, Atom Computing and PsiQuantum. Amazon also launched Amazon Braket, a fully managed quantum computing service that gives customers access to hardware from a diverse set of vendors such as IonQ, Rigetti and D-Wave.

It's also possible that the most valuable quantum platforms won't be versatile, horizontal platforms at all; rather, the space could evolve instead to include special-purpose machines, or quantum application-specific integrated circuits (ASICs). Unlike the way things have played out with classical computing, this could mean that quantum computers would be highly specialized integrated hardware and software machines tailored to specific applications, e.g. fluid simulation or fraud detection.

Early use cases may involve quantum systems taking specialized roles as part of a larger classical system, similar to how NVIDIA's graphics processing units (GPUs), which often run alongside an advanced CPU, can be used to offload specific computations for which the GPU is well-suited. In this model, where quantum components are an "accelerator" to classical systems, a credit underwriter might use a quantum processor to handle one of the tasks involved in scoring applicants and might use a different special-purpose quantum processor to perform a piece of a calculation to optimize its borrower portfolio.

For many use cases, the error rates of calculations are still too high for developers to do more than hone their coding chops on quantum simulation platforms, waiting until quantum computers start to really work at scale. Quantum simulators, such as QMware, make quantum software algorithms and applications believe they are running on actual quantum hardware, but they are really running on classical computers pretending to be quantum computers.

In the meantime, to manage some of the timing uncertainty, quantum-related startups can pursue profitable projects with government, corporate and university buyers today as a source of funding and requirements. Like some biotech startups, they can do this while assembling a strong team and seeking an early adopter clientele, progressing through scientific milestones while keeping an eye on future commercial markets.

The hurdles to generally available quantum computers are much like those faced by alternative energy sources: Unlocking the potential will require breakthroughs in hardware design, lower manufacturing costs and a driving force to spur large-scale adoption. And many approaches won't work.

And as with any technology, it is, of course, possible that software developers will find valuable applications for quantum processors that people haven't thought of yet today—just as developers found that GPUs meant to handle graphics processing also excel at training highly parallelized machine learning models.

That said, a broadly useful and effective quantum computer's arrival has the potential to be as disruptive an opportunity as the creation of the Internet or the use of machine learning to make predictions.

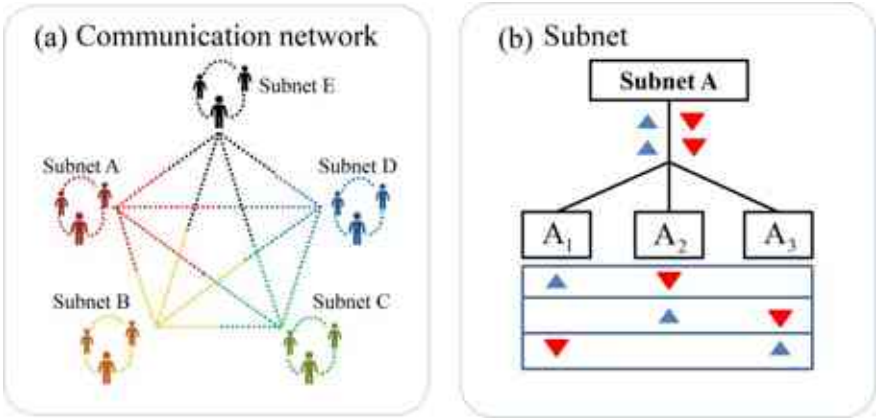
14. A 15-user quantum secure direct communication network

by Chinese Academy of Sciences
https://phys.org/news/2021-09-user-quantum-network.html

Quantum secure direct communication (QSDC) based on entanglement can directly transmit confidential information. Scientist in China explored a QSDC network based on time-energy entanglement and sum-frequency generation. The results show that when any two users are performing QSDC over 40 kilometers of optical fiber, and the rate of information transmission can be maintained at 1Kbp/s. Our result lays the foundation for the realization of satellite-based long-distance and global QSDC in the future.

Quantum communication has presented a revolutionary step in secure communication due to its high security of the quantum information, and many communication protocols have been proposed, such as the quantum secure direct communication (QSDC) protocol. QSDC based on entanglement can directly transmit confidential information. Any attack of QSDC results to only random number, and cannot obtain any useful information from it. Therefore, QSDC has simple communication steps and reduces potential security loopholes, and offers high security guarantees, which guarantees the security and the value propositions of quantum communications in general. However, the inability to simultaneously distinguish the four sets of encoded orthogonal entangled states in entanglement-based QSDC protocols limits its practical application. Furthermore, it is important to construct quantum network in order to make wide applications of quantum secure direct communication. Experimental demonstration of QSDC is badly required.

In a new paper published in *Light Science & Application*, a team of scientists, led by Professor Xianfeng Chen from State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Physics and Astronomy, Shanghai Jiao Tong University, China and Professor Yuanhua Li from Department of Physics, Jiangxi Normal University, China have explored a QSDC network based on time-energy entanglement and sum-frequency generation (SFG). They present a fully connected entanglement-based QSDC network including five subnets, with 15 users. Using the frequency correlations of the fifteen photon pairs via time division multiplexing and dense wavelength division multiplexing (DWDM), they perform a 40-kilometer fiber QSDC experiment by implying two-step transmission between each user. In this process, the network processor divides the spectrum of the single-photon source into 30 International Telecommunication Union (ITU) channels. With these channels, there will be a coincidence event between each user by performing a Bell-state measurement based on the SFG. This allows the four sets of encoded entangled states to be identified simultaneously without post-selection.



(a) The quantum network is fully connected by five subnets (A, B, C, D and E are represented by red, orange, green, blue, and black, respectively). The dotted lines between the subnets (10 links with different colors) are the correlated time-energy photon pairs between the subnets. (b) Every subnet (such as subnet A) is equipped with a 1×3 beam splitter and a delay controlling module, which splits a frequency-correlated entangled photon pair (red and blue signs) and sends them to three users randomly.

It is well known that the security and reliability of the information transmission for QSDC is an essential part in the quantum network. Therefore, they implemented block transmission and step-by-step transmission methods in QSDC with estimating the secrecy capacity of the quantum channel. After confirming the security of the quantum channel, the legitimate user performs encoding or decoding operations within these schemes reliably.

These scientists summarize the experiment results of their network scheme:

"The results show that when any two users are performing QSDC over 40 kilometers of optical fiber, the fidelity of the entangled state shared by them is still greater than 95%, and the rate of **information** transmission can be maintained at 1 Kbp/s. Our result demonstrates the feasibility of a proposed QSDC network, and hence lays the foundation for the realization of satellite-based long-distance and global QSDC in the future."

"With this scheme, each user interconnects with any others through shared pairs of entangled photons in different wavelength. Moreover, it is possible to improve the information transmission rate greater than 100 Kbp/s in the case of the high-performance detectors, as well as high-speed control in modulator being used" they added.

"It is worth noting the present-work, which offers long-distance point-to-point QSDC connection, combined with the recently proposed secure-repeater quantum network of QSDC, which offers secure end-to-end communication throughout the quantum Internet, will enable the construction of secure quantum network using present-day technology, realizing the great potential of QSDC in future communication." the scientists forecast.

15. UK Companies Tout Major Step Toward Universal Quantum Operating System

by Matt Swayne
https://thequantumdaily.com/2021/09/23/uk-companies-tout-major-step-toward-universal-quantum-operating-system/

A consortium led by Cambridge-based quantum computing software company Riverlane and the National Physical Laboratory (NPL) has developed an open-source hardware abstraction layer (HAL) that makes software portable across different quantum computing hardware platforms.

The HAL is designed to be portable across four leading qubit technologies: superconducting qubits, trapped-ion qubits, photonic systems and silicon-based qubits. It will allow high-level quantum computer users, such as application developers, platform and system software engineers, and cross-platform software architects, to write programs for quantum computers portable to these four qubit technologies while maximising performance.

Devising the HAL required collaboration between a large number of players in the UK quantum ecosystem, which were brought together by a £7.6M project funded by the UK government's Industrial Challenge Strategy Fund. Alongside Riverlane and NPL, the consortium includes the UK's quantum hardware companies, SeeQC, Hitachi Europe, Universal Quantum, Duality Quantum Photonics, Oxford Ionics, and Oxford Quantum Circuits, as well as UK-based chip designer, ARM.

The aim is for quantum computer users to be able to implement applications that require the fastest classical/quantum interaction. Previous high-level HALs do not support these types of applications, particularly not across very different

qubit types. The consortium's new, multi-level HAL goes deep into the quantum computing stack, allowing users to take advantage of advanced hardware capabilities for improved performance. This means a developer can focus on the algorithm, rather than the hardware specific implementation, and that the algorithm is portable across different quantum technologies. In the future, the HAL will also provide support for advanced features, such as compiler optimisations, measurement-based control, and error correction.

The HAL will form the backbone of Riverlane's highly innovative quantum operating system, Deltaflow.OS. Dr Leonie Mueck, Chief Product Officer of Riverlane, said: "There are many different evolving systems in the quantum ecosystem and we need an interface that is independent of the hardware to make programs portable. We are therefore delighted to have reached this important milestone. Our HAL effectively allows programmers to 'write once, run anywhere', ensuring the widest possible use of our consortium's technologies and opening up the ecosystem to new players, generating additional commercial opportunities."

Dr Ivan Rungger, Senior Research Scientist of the National Physical Laboratory (NPL), said: "This is the first time that such a diverse group of hardware and software companies have come together to build an open HAL specification and release it publicly. Our aim is to reduce the barrier for non-experts to access quantum technology and to accelerate the pathway to quantum advantage."

This first specification of the HAL is 'version 0 'and is freely accessible on Github. The consortium is seeking feedback from the quantum community, with the eventual aim of including the concepts into an international standard on which the community can build.

Abhishek Agarwal, Research Scientist of the National Physical Laboratory (NPL), continued: "We encourage quantum computer users to try out the HAL. Anyone can implement the HAL and try out their algorithms on qubit emulators. We welcome input to improve the specification further."

The HAL represents an important next step in building a quantum ecosystem that is open to everyone. In this dynamic industry, APIs, backends and interfaces are most effective when they are defined with both hardware companies and users in mind to benefit everyone in the community. This is the philosophy that the HAL is based on. This breakthrough will also help accelerate the commercialisation of the UK quantum technology sector.

16. Physicists Found a New Way to Control Quantum Systems

by Brad Bergan
https://interestingengineering.com/physicists-found-a-new-way-to-control-quantum-systems

Quantum computing has hit a calculation snag.

This is why a research team has described new techniques for effectively controlling the building blocks of quantum computing, taking a substantial step toward a viable way of transforming computers into machines with next-gen accuracy and utility, according to a recent study published in the journal *Nature*.

And if a reliable quantum computing system becomes a reality, it could, among other things, revolutionize modern medicine.

Quantum computing logic gates experience early errors

Physicists David Wineland and David Allcock are founders of the novel Oregon Ions Laboratory, recently formed in the basement of Williamette Hall at the University of Oregon. There are 10 other authors of the new paper, which bases its findings on an experiment carried out at the National Institute for Standards of Technology in Boulder, Colorado. Both Wineland and Allcock have worked at the Colorado lab, and have continued their work on his project since arriving at the UO in 2018. But the new techniques employ trapped-ion quantum bits (also called qubits) in quantum computing and simulations. Working with these might presage major enhancements in the operation of quantum computers, which, as of writing, remain far too unreliable to serve as effective tools, according to a press release on the study.

Put another way, quantum computers have a flaw that scientists suspect is not inherent to the technology. But for now, the logic gates of quantum computers, which perform the fundamental logic functions in computing, "are really bad," said Allcock in the release. "They fail about 1 percent of the time. You can do about 100 (operations), then you get garbage out." In fact, the entire experimental field of quantum computing is limited by these errors, which means "we can't do lengthy calculations or simulations of practical value on our machines," said Wineland, in the release. A major checkpoint for the technology will be to make the logic gates capable of 10,000 operations without experiencing an error, and then adding layers of backup checks to service the issues when they happen.

Quantum computing systems could upgrade drug development methods

"We want to get to that point," said Allcock. "Then you can use quantum computers for something useful. Right now they're just toys." Wineland compares trapped ions to a bowl of marbles possessing magnetic properties. Physicists can manipulate the ions with varying methods, some of which involve lasers, explained Allcock. But lasers are highly sophisticated, complex, and expensive, which makes logic gates a less pricey alternative that is also more practical, since they can be created with integrated circuits. "What we did here is show these techniques work as well as anyone has done logic gates before," said Allcock.

Both IBM and Google have deployed armies of engineers to solve problems like this. Meanwhile, academics are sidestepping some problems to find better, more fundamental techniques to circumvent the issues. "We've shown you can do it a technically simpler way," said Allcock. And, if engineers and physicists can forge quantum computers with the reliability needed to operate at large capacity calculations, they might simulate other systems, like the behavior of a molecule proposed for new drug therapies. This could cut the need to synthesize a new drug out of the development process of drug research. "There are some very practical, useful outcomes," said Wineland on the potential for quantum computers. "We're just scratching the surface."

17. India-based Infosys Cobalt and Amazon Braket Collaborate to Enable Businesses to Begin Exploring the Potential of Quantum Computing

by James Dargan
https://thequantumdaily.com/2021/09/22/india-based-infosys-cobalt-and-amazon-braket-collaborate-to-enable-businesses-to-begin-exploring-the-potential-of-quantum-computing/

Infosys, a global leader in next-generation digital services and consulting, today announced a strategic collaboration with Amazon Web Services (AWS) to develop quantum computing capabilities and use cases. Infosys will use Amazon Braket to explore and build multiple use cases in quantum computing as part of Infosys Cobalt cloud offerings. Amazon Braket is a fully managed quantum computing service that helps scientists and developers get started with the technology and accelerate research and discovery.

Infosys will look to build, test, and evaluate quantum applications on circuit simulators and quantum hardware technologies using Amazon Braket. This will enable researchers and developers to experiment and study complex computational problems as quantum technologies continue to evolve. Enterprises will get access to use cases for rapid experimentation and can explore how quantum computing can potentially help them in the future in a variety of areas, assess new ideas and plan adoption strategies to drive innovation. The use of Amazon Braket by Infosys aims at getting businesses ready for a future where quantum computers will impact business.

The Infosys Center for Emerging Technology Solutions (iCETS), which focuses on the incubation of next-generation services and offerings, is using Amazon Braket to develop quantum computing use cases in vehicle route optimization, fraud detection, and more. Infosys is also exploring partnership opportunities with startups in the quantum computing space through the Infosys Innovation Network (IIN). This collaboration further bolsters Infosys Cobalt, a set of services, solutions, and platforms for enterprises to accelerate their cloud journey. It offers 14,000 cloud assets and over 200 industry cloud solution blueprints.

Ravi Kumar S, President, Infosys, said, “Infosys continues to be at the forefront of exploring and bringing new technologies to clients. Through our use of AWS in this space, we are bringing together the power of Amazon Braket and Infosys Cobalt to help enterprises build quantum computing capabilities and use cases to accelerate their cloud-powered transformation. We are exploring a variety of use cases from the logistics, finance, energy, and telecom sectors that can help clients evaluate future benefits and value that quantum computing could bring to their business. Enterprises can look forward to solving their various complex computational challenges with Infosys Cobalt and Amazon Braket.”

Matt Garman, Senior Vice President of Sales & Marketing at Amazon Web Services, Inc, said, “Quantum Computing is an area of intense research, and a number of businesses around the world are asking about its timeline and the opportunities that it could open. At this stage, it’s important to be aware and evaluate the potential future impact of quantum computing. Infosys, a long-standing for AWS Premier Consulting Partner, has experience in incubating

emerging technology solutions. We see this collaboration as an important step towards setting the right expectations when discussing business problems with customers where quantum computing could have a role."

18. Quantum cryptography Records with Higher-Dimensional Photons

by VIENNA UNIVERSITY OF TECHNOLOGY
https://www.eurekalert.org/news-releases/929244

Quantum cryptography is one of the most promising quantum technologies of our time: Exactly the same information is generated at two different locations, and the laws of quantum physics guarantee that no third party can intercept this information. This creates a code with which information can be perfectly encrypted.

The team of Prof. Marcus Huber from the Atomic Institute of TU Wien developed a new type of quantum cryptography protocol, which has now been tested in practice in cooperation with Chinese research groups: While up to now one normally used photons that can be in two different states, the situation here is more complicated: Eight different paths can be taken by each of the photons. As the team has now been able to show, this makes the generation of the quantum cryptographic key faster and also significantly more robust against interference. The results have now been published in the scientific journal *Physical Review Letters.*

19. Action, not talk, needed to realise Australia's quantum opportunity

by Tim Watts
https://www.innovationaus.com/action-not-talk-needed-to-realise-australias-quantum-opportunity/

The announcement of the AUKUS security partnership by leaders of the United States, United Kingdom, and Australia has triggered a flood of op-eds about the implications of the Morrison Government's decision to reboot its submarine acquisition program for a third time using US nuclear-powered technology.

However, as a tech geek it was the passing reference to trilateral co-operation on cyber capabilities and emerging technologies in the announcement that piqued my interest.

Australia, the US, and the UK already work closely together on operational cyber security matters within the Five Eyes intelligence network. This co-operation and information sharing is overwhelmingly in our national interest and anything we can do to deepen it is warmly welcomed.

The implications of the co-operation on emerging technologies flagged in the announcement are less clear. So far, details are scant.

It's easy to use references to emerging technologies like artificial intelligence and quantum computing as buzzwords, adding a "visionary" or "thought-leading" flavour to an announcement. It's harder to deliver substantive action.

Behind the government marketing hype, Australia's once pioneering quantum computing industry is drifting and we are falling behind.

When Professor Michelle Simmons visited Parliament House in 2018 to spruik her work in quantum computing as the Australian of the Year, we were ranked sixth among the nine largest economies actively investing in quantum technology.

Quantum computing is undoubtedly a tantalising technology. While it's infamously difficult to describe how it works, as an enabling technology a thriving quantum computing industry could be a productivity boon across the Australian economy.

Australian industries as diverse as battery manufacturing, urban management, green steel production, and biomedical science could all become more productive with help from quantum computing.

A recent CSIRO report conservatively estimated quantum computing could create 16,000 new jobs and be worth $4 billion dollars to the Australian economy by 2040, comparable to current estimates of Australia's wool and wheat industries.

Despite the hopes of public relations managers around the world however, technology industries are not built on buzzwords in media statements and press conferences alone.

In the wake of COVID-19 we've seen a slew of governments make multibillion-dollar investments in their domestic quantum computing sectors as part of their economic reconstruction plans; Germany announced a $3.2 billion investment in quantum computing, France a $2.9 billion investment, and China plans to spend $14 billion.

Just this year, both the Australian Strategic Policy Institute and the Australian Information Industry Association released major reports outlining the opportunity and warning that government inaction risks letting it slip through our fingers once again.

According to ASPI, investment in the sector by China, the US, France, Germany, the EU, India, and Russia now exceed Australian investment in quantum by factors of up to 100:1.

When quantum computing researchers meet with Australian politicians today, they tell the story of a national brain drain as Australian quantum talent decamps to more accommodating nations. To countries with governments that have a vision for their quantum computing industries and an investment plan to match it.

Quantum computing risks becoming the latest in a long line of stories where Australian smarts make early breakthroughs in an emerging technology, only to see the commercial returns and the associated jobs realised overseas.

Australia lacks even a national strategy for developing its domestic quantum industry, let alone an investment roadmap to match that of other countries competing for our talent.

The US and the UK are not so complacent. Both nations have significant quantum computing strategies and investment commitments.

The United States will invest around $US 1 billion in quantum computing in 2021. In the UK, investment in the National Quantum Technologies Programme surpassed £1 billion ($A1.8b) in 2019.

Leaders in the UK have already begun to discuss how AUKUS nations could share emerging technology platforms, rather than incurring the costs of duplication. This has potentially significant implications in quantum computing.

But we need a national strategy to guide decisions about which platforms we are happy to use in the US and UK, and which platforms we need to invest in to host ourselves so that we can realise broader benefits for the development of our domestic quantum computing industry.

We won't find the answers to these questions in consultations with the UK and the US. We need to determine them ourselves based on our own ambitions. If we want to realise the benefits of emerging technologies like quantum computing, we can't just talk about them with our international partners, we need the government to act.

Sharing in the benefits of these investments as users of this technology is all well and good. But surely we can aspire to more for ourselves.

We must ask ourselves whether, in this rapidly evolving geostrategic environment, we are content to be technology takers, with our fate determined by the investment and design decisions of governments and companies beyond our shores.

Or, whether we should aspire to become technology makers, shaping our own future.

If we aspire for more, we need to ask more of our government.

20. Why quantum computing is a security threat and how to defend against it

by Ian Barker
https://betanews.com/2021/09/20/quantum-computing-security-threat-defend-qa/

Quantum computing offers incredible computing power and is set to transform many areas such as research. However, it also represents a threat to current security systems as cracking passwords and encryption keys becomes much easier.

So quantum is a security threat, but is there a solution to making systems safer? We spoke to David Williams, CEO of symmetric encryption specialist Arqit, to find out.

BN: Why are current encryption techniques no longer adequate?

DW: First, public key cryptography was not designed for a hyper-connected world, it wasn't designed for an Internet of Things, it's unsuitable for the nature of the world that we're building. The need to constantly refer to certification providers for authentication or verification is fundamentally unsuitable. And of course the mathematical primitives at the heart of that are definitely compromised by quantum attacks so you have a system which is crumbling and is certainly dead in a few years time.

A lot of the attacks we've seen result from certifications being compromised, certificates expiring, certificates being stolen and abused.

But with the sort of computational power available from a quantum computer blockchain is also at risk. If you make a signature bigger to guard against it being cracked the block size becomes huge and the whole blockchain grinds to a halt.

BN: Where did you start to look for a solution?

DW: The person who solves this will become very successful, so in 2017 we began an innovation journey. The tech that we had back then most definitively did not work, it didn't solve the problem. What we now have is a product which is called **Quantum Cloud**. It's just a lightweight software agent that's 200 lines of code that can be delivered from the cloud and it can be downloaded into any device. We can put it into an IoT sensor, or a battleship, it doesn't matter, it's the same software for all devices.

What that software does is it creates keys for groups of devices that want to communicate securely, so it could be two or 20 or 2000 devices, and they all undergo a process whereby they create a brand new symmetric encryption key, which they then use to communicate securely. We know that symmetric encryption key is computationally secure. A symmetric encryption key is just a long random number, and even a quantum computer in future will not be able to crack it in less than billions of years. Symmetric encryption keys have been used for decades, delivered by human courier, and therefore the algorithm to use such keys is already built into the world's software systems which means there's no great change required for the world to adopt the use of this technology.

We didn't invent symmetric encryption keys, we invented a way to distribute them securely.

BN: Can you give us an idea of how this works?

DW: Imagine two end points in London and New York who want to create a secure channel. Each device talks to a data center in its city. In each location there are Hardware Security Modules (HSMs) which have identical sets of the encryption key data. That data is put there by 'satellites' which use a quantum protocol to deliver that information in a method that we can demonstrate is provably secure.

Think of the data centers as buckets, three times a day the satellites throw some random numbers into the buckets and all data centers end up with an identical bucket full of identical sets of random information. So, the endpoints talk to the data centers, which have a conversation and they agree on some information or clues to send in common to the end points, without actually knowing what that information is. In a very clever mashup of those clues, and the existing data that they have on their devices, the end points then create simultaneously a brand new random number.

BN: Is this available today?

DW: The satellite technology is still a couple of years away, currently the root source of random numbers is delivered to data centers by a random number generator in a data center, through some terrestrial mechanisms, which is regarded by our customers as secure today. It's not quantum safe yet, but the network gets upgraded in two years time when the quantum satellites launch and the whole thing becomes quantum safe.

BN: How will it tie in with a zero trust world?

DW: Conventionally with satellite quantum encryption, you can either be zero trust or you can be global, you can't be both. Well that makes the whole thing a bit pointless because the internet's global. Our technology is simultaneously

zero trust and global. So, in our protocol the satellite is never trusted with the key, an individual receiver is never trusted with the key. It is a zero trust system. But secondly, the endpoint software adds another layer of zero-trust functionality. The data centers never have the key, the key is never created somewhere else and distributed. The key is created locally on the device, and therefore there is no other device in the network which we're trusting with the key. Therefore, the software protocol is also zero trust.

BN: Will the end user logging into their bank or VPN see any difference?

DW: It's unlikely that a consumer will ever see the operation of our new software, you won't see it sitting on your device called 'Arqit's product', it will be baked into other people's applications and it will be a seamless experience for the average customer.

BN: Are there wider applications for the technology?

DW: One of the things we're most excited about is JADC2 (Joint All-Domain Command and Control), which is basically the military Internet of Things. This involves lots of devices that need to operate in dynamic environments. You can't possibly give every single device that you might feasibly want to communicate with a set of keys to cope with every possible scenario it's simply impossible. And in JADC2 we have to rely currently on old fashioned public key cryptography.

But if every device can just download the lightweight quantum cloud agents, then as soon as you agree that drone needs to talk to that satellite, which needs to talk to that other commander, they just set up brand new key dynamically in real time. We can create unbreakable and trustless keys in the moment that they needed and we can change the access rights.

Of course the same problem is also solved in the enterprise and for consumer devices. So yes, the application of our technology is everything, everywhere. There is no application we've ever thought of where the technology can't make things stronger and simpler.

21. Twisted light makes for breakthrough quantum computer chip

by Michael Irving
https://newatlas.com/computers/twisted-light-quantum-computer/

Quantum computers have the potential to drastically outperform traditional computers, but for now they're mostly limited to labs and big experimental setups. Japanese researchers have now made a step towards more accessible quantum computing devices, finding a way to "twist" light at room temperature.

Some types of quantum computers use photons as their data-carrying particles. To encode information into these photons, electrons in a device are manipulated into a certain state that represents either a zero or one. When these electrons then interact with certain light-emitting materials, they pass this information onto photons, which can store and transmit it.

One emerging method of encoding data in quantum computers is through what's known as valley-polarized light. Essentially, electrons can exist in several different energy bands, with "valleys" between them where their energy is low. When electrons in these valleys produce light in a device, they create a circular pattern of polarized light that can twist either left or right (a property known as chirality), which has strong potential for quantum information storage and transmission.

The problem is, this kind of twisting, chiral, valley-polarized light can usually only be generated using strong magnets and temperatures approaching absolute zero, so it remains in the realm of big lab setups. But in the new study, researchers from Nagoya University found a way to produce this light at room temperature, without magnets.

In early experiments, the team created a semiconductor device to produce the light at temperatures down to -193 °C (-315 °F). They observed that chiral light was produced at warmer temperatures in some sections of the device – but only where the substrate had been strained during synthesis. Where the substrate had undergone no strain, chiral light wouldn't be produced until the temperature dropped drastically.

To test the hypothesis that strain played a part, the team then created a new device, made of tungsten disulfide on a plastic substrate. They bent the device to apply strain to the material, and found that it produced an electric current in the same direction as the strain. That in turn generated valley-polarized light, at room temperature. To switch the light to move in the opposite direction, an electric field can be applied.

"Our use of strained monolayer semiconductors is the first demonstration of a light-emitting device that can electrically generate and switch right- and left-handed circularly polarized light at room temperature," says Taishi Takenobu, co-lead author of the study.

The team says that this breakthrough could lead to more powerful consumer-level quantum computing devices. Future work will focus on optimizing the system to move towards that possibility.

The research was published in the journal *Advanced Materials*.

22. NSA and CISA Publish Kubernetes Hardening Guidance

by Mostafa Radwan
https://www.infoq.com/news/2021/09/kubernetes-hardening-guidance/

The National Security Agency(NSA) in partnership with the Cybersecurity and Infrastructure Security Agency(CISA) recently published the Kubernetes Hardening Guidance, a technical report focused on securing Kubernetes environments.

The report identifies the common areas of Kubernetes security risks: supply chain, malicious actors, and insider threats. It aims to educate engineers to avoid common misconfiguration issues and safeguard applications.

The guidance suggests that supply chain risks are hard to mitigate and can emerge in the container building cycle or infrastructure provisioning especially in cloud environments.

Some of the recommendations in the report to build secure container images include using trusted repositories, detecting vulnerabilities in images by using a container image scanner, and running containers and pods with the least privileges possible.

One approach mentioned in the report to integrate image scanning is by using an admission controller. A Kubernetes feature that can intercept requests to the Kubernetes API server before the creation of an object, but after authentication and authorization. That way, deployments that don't comply with the organization's security policy are blocked.

The report also underlines that malicious actors are keen to compromise Kubernetes clusters, especially on the public cloud for many reasons including stealing data and computation power or mining cryptocurrency.

There are many recommendations in the report to mitigate such risks such as encrypting data in transit using Transport Layer Security(TLS) and at rest including secrets. Also, using network policies and firewalls to limit the blast radius of a compromise.

The report refers to running non-root containers as well as rootless container engines. That way, a threat actor who can compromise a particular container won't be able to escape with all of the root capabilities of a host machine. By default, many applications in containers run as the root user even though little or no access to the underlying host is required.

In addition, the guidance underscores the risk of insider threats. Those are users, administrators, or cloud service providers with special access privileges who can abuse such privileges and compromise the Kubernetes environment.

Some of the recommendations in the report to mitigate such risk include using strong authentication and authorization utilizing RBAC to limit the access of users and administrators. Also, disabling anonymous requests that are enabled by default in Kubernetes can limit the attack surface.

The guidance encourages administrators to stay up to date when it comes to patches, updates, and upgrades. In addition, it highlights the importance of regularly checking the Center for Internet Security(CISA) benchmarks for securing software as well as best practices.

Kubernetes is open-source software that automates the deployment, scaling, and management of applications. It's the de facto standard for managing application containers at scale. Google donated the technology to the Cloud Native Computing Foundation (CNCF) in 2015. CNCF is part of the Linux Foundation dedicated to the advancement of cloud-native software, community, and ecosystem.

The 59-page technical report is part of NSA's library which includes many cybersecurity advisories related to networking, 5G Infrastructure, cloud vulnerabilities, and more.

23. A New Wave of Malware Attack Targeting Organizations in South America

by Ravie Lakshmanan
https://thehackernews.com/2021/09/a-new-wave-of-malware-attack-targeting.html

A spam campaign delivering spear-phishing emails aimed at South American organizations has retooled its techniques to include a wide range of commodity remote access trojans (RATs) and geolocation filtering to avoid detection, according to new research.

Cybersecurity firm Trend Micro attributed the attacks to an advanced persistent threat (APT) tracked as APT-C-36 (aka Blind Eagle), a suspected South America espionage group that has been active since at least 2018 and previously known for setting its sights on Colombian government institutions and corporations spanning financial, petroleum, and manufacturing sectors.

Primarily spread via fraudulent emails by masquerading as Colombian government agencies, such as the National Directorate of Taxes and Customs (DIAN), the infection chain commences when the message recipients open a decoy PDF or Word document that claims to be a seizure order tied to their bank accounts and click on a link that's been generated from a URL shortener service like cort.as, acortaurl.com, and gtly.to.

"These URL shorteners are capable of geographical targeting, so if a user from a country not targeted by the threat actors clicks on the link, they will be redirected to a legitimate website," Trend Micro researchers detailed in a report published last week. "The URL shorteners also have the ability to detect the major VPN services, in which case, the shortened link leads the users to a legitimate website instead of redirecting them to the malicious link."

Should the victim meet the location criteria, the user is redirected to a file hosting server, and a password-protected archive is automatically downloaded, the password for which is specified in the email or the attachment, ultimately leading to the execution of a C++-based remote access trojan called BitRAT that first came to light in August 2020.

Multiple verticals, including government, financial, healthcare, telecommunications, and energy, oil, and gas, are said to have been affected, with a majority of the targets for the latest campaign located in Colombia and a smaller fraction also coming from Ecuador, Spain, and Panama.

"APT-C-36 selects their targets based on location and most likely the financial standing of the email recipient," the researchers said. "These, and the prevalence of the emails, lead us to conclude that the threat actor's ultimate goal is financial gain rather than espionage."

24. Building a quantum future

by National Quantum Computing Centre

https://physicsworld.com/a/building-a-quantum-future/

Construction will soon be starting on the world's first national laboratory to be dedicated to quantum computing. With funding of £93m over the next five years, the primary objective of the UK's National Quantum Computing Centre (**NQCC**) is to accelerate the scale-up and exploitation of practical quantum computers. The NQCC will be built in Harwell, Oxfordshire, alongside several other top-tier scientific facilities operated by the Science and Facilities Technology Council (STFC), and is due to open in 2023.

One of the NQCC's key deliverables is to demonstrate a quantum computer with more than 100 qubits by 2025, which means that the NQCC team has already started to commission its first tranche of R&D projects. "The building is important, but we couldn't wait for it to be finished because the technology is evolving rapidly and our international competitors and collaborators are moving forward at pace," says the NQCC's director Michael Cuthbert. "We need to

do something tangible, to get started with some development work that we can learn from and that will shape our future technology programme."

The initial objectives and priorities for the NQCC have emerged from a **detailed technology roadmap developed by around 20 of the UK's leading quantum experts over the last two years**. The roadmap highlights current activities in quantum computing, identifies the key strengths of the UK's quantum community, and evaluates the maturity of different technology platforms and their potential over the next 10 years. Cuthbert and his team have now translated the outcomes of that roadmap into a series of work packages across software, hardware and application development that are now being awarded competitively to both academic and industrial partners.

The NQCC is fortunate to have access to a thriving quantum community of research groups and start-up companies, as well as larger industrial organisations that could become important end-users for future quantum computers. That collaborative ecosystem has been fostered in large part by the UK's National Programme for Quantum Technologies, which has supported technology hubs in quantum sensing, imaging, communications and computing since 2014. While the UK is traditionally seen as strong in academic research but weaker on commercial exploitation, Cuthbert points out that this co-ordinated activity has already spawned 41 start-up companies that are already capitalizing on the emerging market for quantum technologies. "Between them they have raised more than £135m in investment funding," he says. "They are developing robust business models and making international connections that could enable them to become the major global players of the future."

A primary objective for the NQCC will be to accelerate the growth of that quantum economy by speeding up the migration of scientific research into commercial exploitation. "There is often a gap in skills and resources when going from purely academic research into the commercial sector, and the NQCC will be aiming to bridge that gap," explains Cuthbert. As well as incubating new start-ups and making connections with industry, an important role for the NQCC will be to nurture training and skills development – enabling academics to move into the commercial world and industry professionals with more general engineering and computing backgrounds to gain the knowledge they need to work with quantum technologies.

When the building opens in 2023, it will offer collaborative working spaces along with laboratories for testing devices and building prototype quantum computers. As well as pursuing its own R&D projects, the NQCC will continue to commission external R&D from research groups and industrial partners, and in some cases will co-develop specific technologies or applications. "We want to accelerate our own roadmap, as well as those of the academic and industrial communities," says Cuthbert. "We don't want to duplicate work that's being done very successfully elsewhere."

Cuthbert is acutely aware that the path towards useful quantum computing will be long and challenging. The initial focus for the centre is to demonstrate a working quantum computer with more than 100 qubits, which will operate in the so-called noisy intermediate-scale quantum (NISQ) regime. Such early machines are vital for demonstrating capability and showing the promise of quantum computers, but they will not be able to challenge the performance of today's high-performance supercomputers.

"It is a much longer roadmap, perhaps 10 to 15 years, towards large-scale machines that will realize the fully transformative power of quantum computing," says Cuthbert. "Modest-scale machines are part of the journey to getting there, and that long-term endeavour is one of the reasons we need a national facility."

A crucial element of that long-term vision is to catalyse a user community that will help to identify useful applications for quantum computers. "Until now we've mostly focused on technology development, but ultimately quantum computing needs to deliver applications that make a real difference across different economic sectors," he says. "The

NQCC has an important role to play in providing access to third-party machines, particularly for the research community, and then providing applications support to develop a user community that can really explore the value that can be derived from quantum computing."

For that reason the NQCC is now commissioning a number of smaller projects to develop use cases for today's prototype machines. These projects will explore the impact that quantum computing might have in different business sectors and research fields, and attempt to translate complex problems in those different domains into tasks that quantum computing can address. "The outcomes from those projects will go to the heart of whether quantum computing is just a science project, or whether it will really deliver on the potential that everyone is talking about," comments Cuthbert.

Meanwhile, in its bid to build a prototype machine with more than 100 qubits, the NQCC will initially focus its efforts on two technology platforms – superconducting qubits and trapped-ion systems – that the roadmap identified as having the most chance of early success. However, Cuthbert is quick to point out that other technologies could also play an important role in the future. "We have said all along that it's far too early to be picking winners. This was about identifying where we should start, rather than saying that this is the one and only technology decision we will ever take," he says. "We will be continuously assessing that roadmap and the ongoing development of alternative platforms, and figuring out how to bring frontier development work into the NQCC programme."

The most fundamental challenge for the developers of future quantum computers will be to scale the number of qubits without scaling their inherent noise. Current prototypes incorporate some level of error mitigation to reduce the effects of noise, but many more qubits will be needed to enable full-scale error correction. Some estimates suggest that as many as 10,000 qubits might be needed provide one operational qubit in a general-purpose quantum computer.

Another pressing priority will be to find a way to scale the control system and associated engineering infrastructure along with the devices themselves. The quantum computers that have already been demonstrated by the likes of Google and IBM require thousands of coaxial cables to switch and readout the state of each individual qubit, while trapped-ion systems require optical measurements that become increasingly complex as the machine gets larger.

"We will need some major technology breakthroughs to allow us to address the qubits more quickly and efficiently," says Cuthbert. "Many groups are already working on technologies to multiplex the signals that are used to control the qubits, and one major step forward would be to integrate some of the control systems into the cryogenic chamber so they are much closer to the physical qubits."

Overcoming those technology hurdles will require not just fundamental breakthroughs in quantum physics, but also significant innovations in systems engineering and computational science. "We need a whole range of skills and knowledge to deliver the future roadmap for quantum computing," says Cuthbert, who has just embarked on an ongoing recruitment process that will see 65 people join the NQCC by the time the building opens in 2023. "We need scientists with an academic background in quantum computing who want to play a role in translating the technology, as well engineers and computer scientists who want to work with us to understand and shape the future of quantum computing."

25. Pivoting into Quantum Computing & Solving Industry Challenges with Cambridge Quantum

by Quantum London
https://medium.com/quantum-london/pivoting-into-quantum-computing-solving-industry-challenges-with-cambridge-quantum-6786b94d6cc4

We're always excited to flag up events which fit out mission of explaining the business impact of quantum computing. This one includes many of our favorite quantum people.
It is NOT a Quantum London event so please pay close attention to the information and RSVP requirements on the event website.

During this panel discussion, Danika will talk about how her interest in quantum mechanics inspired her to move into the quantum computing industry. Danika's background in fintech and data science has helped her bring Cambridge Quantum's (CQ's) solutions to the marketplace, especially in regards to CQ's most recent advancements in quantum Monte-Carlo integration and optimization . This panel is being held in joint partnership with the Minnesota Quantum Computing Meetup.

Danika Hannon's a Relationship Manager with CQ. In her role, she grows client relationships and finds new partners who want to work with CQ to tackle their most intriguing challenges by leveraging CQ's applications in quantum chemistry, quantum machine learning, optimization, cybersecurity and quantum natural language processing.

26. China advances industrial application of quantum technology

by Xinhua
https://www.china-daily.com.cn/a/202109/19/WS614673d4a310cdd39bc6a483.html

With a height of about one meter and weight of less than 100 kg, a miniaturized quantum satellite ground station caught the eyes of audiences at the 2021 Quantum Industry Conference held Saturday in Hefei, capital of East China's Anhui province.

"Such ground station is light and portable, and can be installed within 12 hours, allowing users in remote areas to use quantum communication conveniently," said Zhou Lei, project director of quantum in QuantumCTek Co Ltd, a leading quantum company based in Anhui.

The company also displayed a quantum key distribution equipment about the same size of a laptop, which can greatly reduce the cost of quantum network building and maintenance.

In recent years, China has achieved a series of breakthroughs in quantum technology, including the world's first quantum satellite, a 2,000-km quantum communication line between Beijing and Shanghai, and the world's first optical quantum computing machine prototype.

"With the active participation of leading enterprises and the guidance of government, an industrial chain that covers the equipment, network, safety and standards of quantum communication has been basically formed in China," said Pan Jianwei, a renowned quantum scientist from the University of Science and Technology of China, at the conference.

Hefei, a hub for China's quantum technology, is home to over 20 quantum technology enterprises and achieved an output value of some 430 million yuan (about $66.5 million) in 2020.

"The quantum information technology is to be further integrated, convenient and low-cost, allowing more people to have access to it," said Zhou of QuantumCTek.

China Telecom Quantum Technology Co Ltd has tried out the quantum encryption calls in 15 provinces since June and has garnered some 10,000 users, said Wang Jian, manager of the research and development department of the company.

"The users can have secure calls and messages encrypted with quantum keys after inserting a SIM card and installing a related app, which can ensure information security," said Wang.

Besides quantum communication, quantum precision measurement and quantum computation have also seen great breakthroughs in industrial applications.

Produced by CIQTEK Co Ltd, a quantum precision measurement instrument called quantum diamond atomic force microscope can achieve nanoscale high spatial resolution and single spin ultra-high detection sensitivity, which has been applied to study the magnetic and superconducting materials.

"Our products have been used in fields including oil exploration, life sciences and power grids. Since the founding of our company five years ago, the output value has almost doubled every year and the revenue was over 100 million yuan last year," said He Yu, president of CIQTEK, a manufacturer and provider of quantum precision measurement products.

Origin Quantum, a startup focusing on quantum computers and related technologies, launched OriginQ Cloud, a full stack quantum computing service platform on the conference, which can provide quantum computing, simulation training, quantum application development and other services for quantum computing developers and enthusiasts.

"Many of our works are original research, and we are exploring the future commercial model to combine quantum computation with industries including finance, biological medicine and space," said Zhang Hui, general manager of Origin Quantum.

27. Concerned About Quantum Computing Ethics? Start by First Helping to Fix Classical Computing Ethics!

https://quantumcomputingreport.com/concerned-about-quantum-computing-ethics-start-by-first-helping-to-fix-classical-computing-ethics/

We are seeing a number of efforts to examine the topic of quantum computing ethics. Although this is commendable, our view is that guidelines for quantum computing ethics need to be built upon a strong platform of classical computing ethics. **And classical computing ethics are a mess right now!** We don't think efforts to develop quantum computing ethical standards will make any progress until the classical computing side is fixed first. It would be like trying to build a new second story addition on top of a dilapidated single story house that has been neglected for many years.

There are very significant issues in classical computing ethics that need attention including a few examples shown in this list below:

- Update to Section 230 of the Communications Decency Act of 1996
- Computer Crime
- Ethical Use of Facial Recognition
- Data Privacy Protection
- Ethical Use of Social Media
- Intellectual Property Protection
- Misinformation and Deep Fakes

Our feeling is that most, if not all, of the potential ethical issues that can arise with quantum computing will be the same as those existing in classical. Certainly a quantum computer may be able to do some functions more accurately or faster, but we do not think the differences will be drastic enough to substantially change the ethical considerations. For example, we can see how quantum computing might someday make facial recognition a little more accurate than doing it classically, but we can't see how the ethical issues and the possible solutions will be any different.

So you might ask, "What about the potential to break the RSA encryption algorithm using Shor's algorithm to factor a large number with a future quantum computer?" We see this as more of an engineering and operational issue. If someone passes a law saying "Thou Shalt Not Run Shor's Algorithm" we think the bad guys will ignore it. And they certainly won't observe any guidelines that have been written down in a white paper!

There is, of course, substantial activity underway in algorithm development, standards activity, device construction and other research to develop quantum resistant alternatives to the current methods of public key distribution. And there will certainly be a massive upgrade over the next twenty years to our communications infrastructure to adopt these technologies. But this is more a matter of execution rather than proclaiming what is right or wrong.

We are always a proponent of first things first. So if you are concerned about computing ethics, our advice is to spend your time and effort by first working to get the classical side fixed. Not only will that be more productive, but if there are any quantum specific ethical issues that come up in the future, you will be better equipped to address it. You will

have had the experience with working on the classical issues first and the lessons learned there will make resolving the quantum issues faster and easier.

28. First UK Fibre Link Network For Precision Timing to Be Established in UK by Hub Researchers

https://thequantumhubs.com/first-uk-fibre-link-network-for-precision-timing-to-be-established-in-uk-by-hub-researchers/

A ground-breaking new project spearheaded by UK Quantum Technology Hub Sensors and Timing researchers at the University of Birmingham and the National Physical Laboratory (NPL) will see a fibre optic cable installed underneath the University's campus, connecting all the way through to NPL's head office in Teddington, south-west London. This project will mark the first time a fibre optic cable network for precision timing has been extended to such a large area in the UK, paving the way for resilient, highly accurate synchronisation for the future.

Known otherwise as dark fibre, this fibre optic network will essentially be an independent connection that will uniquely use optical amplifiers to simultaneously boost multiple signals, which typically deteriorate every 80 km. Hub researchers are deploying single amplifiers as opposed to placing multiple amplifiers at the same location to prove that performance is not affected by this method, a solution that will save significant time and money.

This network will test both performance and resilience in time and frequency transfer, which would have significant impact on a number of sectors, such as finance and defence. Fibre link technology can only be interfered with if it is physically cut, which would take considerable resource compared to satellite signal spoofing and hacking. Fibre optic cables are also much less susceptible to interferences, as the data is concentrated within the fibre itself. Accuracy is also expected to measure a hundred times more precise than our current national time network.

Researchers will test the possibility of using fibre link networks to support GPS networks in the future. This will represent a step-change in the technology that underpins our current communications network, which in turn is the foundation for many services which make up the UK's critical national infrastructure, such as hospitals, transport and utilities.

The network installation, which will be carried out by Jisc, is currently underway and is scheduled to be completed by October 2021. The network will initially be available for three years, with the potential to become permanent.

"This technology has already been tested in Paris, and I'm excited about the Hub taking the first step in establishing a UK-wide time and frequency distribution network." Dr Jochen Kronjaeger, NPL

"This is a unique opportunity to assess new, interdisciplinary technology with NPL's world-leading experts. Timing advancements may take years to result in real-world system changes, but this new project represents a step forward to fast, secure systems." Dr Michail Antoniou, Quantum radar and timing Hub lead

29. Chinese Research Group Makes Further Improvements in their Quantum Supremacy Experiment; Now at 60 Qubits with 24 Levels

https://quantumcomputingreport.com/chinese-research-group-makes-further-improvements-in-their-quantum-supremacy-experiment-now-at-60-qubits-with-24-levels/

We reported in June that a Chinese quantum research group had developed a superconducting based quantum computer named Zuchongzhi 2.0 and had replicated and surpassed Google's Quantum Supremacy experiment with a circuit that used 56 qubits to calculate random circuits to a depth of 20 levels. This surpassed Google's initial result which used a 53 qubit circuit to a depth of 20 levels. The total number of raw qubits in the Zuchongzhi system is 66, but did not use all of them in their initial experiement. After additional improvements the group has created a Zuchongzhi 2.1 machine and reran the experiment to demonstrate successful operation with 60 qubits to a depth of 24. The group claims that this larger sampling tasks is three orders of magnitude more difficult than what they previous achieved on the Zuchongzhi 2.0 and six orders of magnitude more difficult that Google's original demonstration with their Sycamore processor. It appears that the main improvement in Zuchongzhi 2.1 is in the readout circuitry with the average readout fidelity going from 95.48% to 97.74%. A paper has been posted on arXiv with more details about this experiment and is available here.

30. We Cannot Live Without Cryptography!

by Marcel Blackbeard
https://www.techspot.com/article/2323-cryptography/

You're about to wind up your day and use your smartphone to check what's in your smart fridge to decide if you need to pass by the store or request delivery before you get home. You quickly pay for the purchase using your credit card registered on your account and promptly receive a push notification confirming the purchase and estimated delivery times.

You use your Metro transit card to jump on the bus or subway train to start making your way home, all the while listening to your favorite podcast on Spotify. Once you get home, you pick up your dinner and jump on to a Zoom call with your loved ones, quickly glancing to confirm the green padlock is active and your call is secure.

Your typical day may resemble the above or some aspects of it, but everything that we take for granted in a typical day requires some form of cryptography. A tiny bit of code that keeps us safe in the digital world -- who to trust, who we say we are, was our data tampered with before delivery, or even if we are allowed to access a website.

Yet the word cryptography evokes images of spies (*James Bond* included), secret messages, covert government agencies, conspiracy theories, and wars flood our minds at the mention of 'cryptography.' In fact, movies like "The Da Vinci Code" and "The Imitation Game" revolve around this fascinating science of concealing information.

While we may be content to leave cryptography to the experts and movies, it is all around us. From the moment you unlock your phone in the morning, access a website, make an online payment, watch Netflix, or purchase an NFT.

It's hard to believe, but cryptography has been around for thousands of years. Early cryptography focused on protecting messages during transportation between allies. Modern cryptography matured to verify data integrity, authenticate identities, implement digital signatures, and many others.

.
.
.

31. Juniper Inks Partnership with Quantum Encryption Firm Arqit Quantum

by RAY SHARMA
https://www.thefastmode.com/technology-solutions/20815-juniper-inks-partnership-with-quantum-encryption-firm-arqit-quantum

Arqit Quantum, a leader in quantum encryption technology and Juniper Networks have signed a 'Technology Alliance Partner Connect 'agreement to explore network security technology that will protect against quantum security threats.

Cyber-attackers regularly target networks to disrupt business operations. Arqit and Juniper will explore how network providers can apply quantum secure key-exchange mechanisms to limit interruptions and improve business resiliency.

The increasing use of software-defined networking, and the ability to dynamically provision networks, along with more secure cryptographic key exchanges, offers network providers the opportunity to provide stronger, more active authentication of devices to secure organisations 'data from even a quantum attack.

Under the 'Technology Alliance Partner Connect 'agreement, Juniper and Arqit will work together to explore and test the application of quantum security technologies, including Arqit's innovative platform QuantumCloud, to networks.

32. Competing Visions Underpin China's Quantum Computer Race

by CRAIG S. SMITH
https://spectrum.ieee.org/alibaba-baidu-quantum-computer-race

China and the US are in a race to conquer quantum computing, which promises to unleash the potential of artificial intelligence and give the owner all-seeing, code-breaking powers.

But there is a race within China itself among companies trying to dominate the space, led by tech giants Alibaba and Baidu.

Like their competitors IBM, Google, Honeywell, and D-Wave, both Chinese companies profess to be developing "full stack" quantum businesses, offering access to quantum computing through the cloud coupled with their own suite of algorithms, software, and consulting services.

Alibaba is building solutions for specific kinds of hardware, as IBM, Google, and Honeywell are doing. (IBM's software stack will also support trapped ion hardware, but the company's focus is on supporting its superconducting quantum computers. Honeywell's software partner, Cambridge Quantum, is hardware agnostic, but the two companies' cooperation is focused on Honeywell's trapped ion computer.)

Baidu is different in that it is building a hardware-agnostic software stack that can plug into any quantum hardware, whether that hardware uses a superconducting substrate, nuclear magnetic resonance, or ion traps to control its qubits.

"Currently we don't do hardware directly, but develop the hardware interface," Runyao Duan, Baidu's head of quantum computing, told the 24th Annual Conference on Quantum Information Processing earlier this year. "This is a very flexible strategy and ensures that we will be open for all hardware providers."

Quantum computers calculate using the probability that an array of entangled quantum particles is in a particular state at any point in time. Maintaining and manipulating the fragile particles is itself a difficult problem that has yet to be solved at scale. Quantum computers today consist of fewer than 100 qubits, though hardware leader IBM has a goal of reaching 1,000 qubits by 2023.

But an equally thorny problem is how to use those qubits once they exist. "We can build a qubit. We can manipulate a qubit and we can read a qubit," said Mattia Fiorentini, head of machine learning and quantum algorithms at Cambridge Quantum in London. "The question is, how do you build software that can really benefit from all that information processing power?"

Scientists around the world are working on ways to program quantum computers that are useful and generalized and that engineers can use pretty much straight out of the box.

Of course, real large-scale quantum computing remains a relatively distant dream—currently quantum cloud services are primarily used for simulations of quantum computing using classical computers, although some are using small quantum systems—and so it's too early to say whether Baidu's strategy will pay off.

In the past, Alibaba worked with the University of Science and Technology of China in Hefei, the capital of central China's Anhui province, which currently has the world's most advanced quantum computer, dubbed the Zuchongzhi 2.1, after China's famous fifth century astronomer who first calculated pi to six decimal places. The company is also building quantum computing hardware of its own.

China's most important quantum scientist, Pan Janwei, also worked for Alibaba as scientific advisor. Earlier this year, Pan's team set a new milestone in quantum computation with the 66-qubit Zuchongzhi 2.1. Pan and his team ran a calculation on the device in about an hour and a half, which would take the world's fastest supercomputer an estimated eight years to complete.

Baidu, meanwhile, has been releasing a series of platforms and tools that it hopes will put it ahead when quantum computers eventually become large enough and stable enough to be practical.

Last year, it announced a new cloud-based quantum computing platform called Quantum Leaf, which it bills as the first cloud-native quantum computing platform in China—a bit of semantics apparently intended to put it ahead of Alibaba's cloud division, which began offering a cloud-based quantum platform with the Chinese Academy of Sciences several years ago.

Unlike Alibaba's platform, Quantum Leaf's cloud programming environment provides quantum-infrastructure-as-a-service.

Baidu's cloud-native quantum computing platform Quantum Leaf provides access to the superconducting quantum processing unit from the Institute of Physics, Chinese Academy of Sciences.

Baidu also released Paddle Quantum, a device-independent platform for building and training quantum neural network models for advanced quantum computing applications. It combines AI and quantum computing using the company's deep learning framework called PaddlePaddle—Paddle means PArallel, Distributed, Deep Learning—which has 3.6 million developers and can support hyperscale training models with trillions of parameters.

Paddle Quantum, in turn, can be used to develop quantum neural network models for software solutions. Users can then deploy those models on both quantum processing units or simulators through Quantum Leaf.

Baidu also offers a "cloud-based quantum pulse computing service" called Quanlse, intended to bridge the gap between hardware and software through sequences of pulses that can control quantum hardware and reduce quantum error, one of the biggest challenges in quantum computing.

"We see an increasing number of demands from universities and companies to use our quantum platform and collaborat[e] on quantum solutions, [which] is an essential part of our quantum ecology," a Baidu spokesperson said.

Baidu's quantum activities are largely focused on quantum artificial intelligence, an extension of Baidu's current artificial intelligence activities. Quantum computing is expected to accelerate the development of artificial intelligence both by making models faster but also by allowing compute-intensive models not currently possible on classical computers.

The company established a quantum computing institute in 2018 whose research includes classification of quantum data, which opens the door to quantum machine learning. To classify chemical compounds as toxic or non-toxic, for example, data scientists currently use classical means. But because the underlying data—the molecules and their configurations—is quantum data, it would be faster and more accurate to classify that quantum data directly with a quantum computer.

Quantum information is encoded in the probability distribution of qubit states. That probability distribution is reconstructed by collecting samples with classical means, but the number of samples needed grows exponentially as you add qubits.

"The more you add qubits to your quantum system, the more powerful the system, but the more samples you need to take to extract all useful information," says Cambridge Quantum's Fiorentini.

Existing methods for quantum classification are impractical because hardware and infrastructure limitations restrict the complexity of the datasets that can be applied.

Baidu researchers' new hybrid quantum-classical framework for supervised quantum learning uses what they call the "shadows" of quantum data as a subroutine to extract significant features—where "shadows" here refers to a method for approximating classical descriptions of a quantum state using relatively few measurements of the state.

"If we can get all the key information out of the quantum computer with a very small number of samples without sacrificing information, that's significant," says Fiorentini.

Baidu's hybrid quantum-classical framework, meanwhile, sharply reduces the number of parameters, making quantum machine learning models training easier and less compute intensive.

In the near term, the company says, Baidu is pursuing more efficient and more powerful classical computing resources that can accelerate its AI applications, from training large-scale models to inferencing on the cloud or edge. In 2018, it developed a cross-architecture AI chip called Kunlun, named or the mountain range on the Tibetan plateau that is the mythological origin of Chinese civilization.

Baidu has produced more than 20,000 14-nm Kunlun chips for use in its search engine, Baidu AI cloud and other applications. It recently announced the mass production of Kunlun II, which offers 2-3 times better performance than the previous generation, using the world's leading 7nm process and built on Baidu's own second-generation cross-platform architecture. Kunlun II has a lower peak power consumption while offering significantly better performance in AI training and inferencing. The chip can be applied in multiple scenarios, including in the cloud, on terminal, and at the edge, powering high-performance computer clusters used in biocomputing and autonomous driving.

33. Quantum computing is at an early stage. But investors are already getting excited

by Daphne Leprince-Ringuet
https://www.zdnet.com/article/quantum-computing-is-at-an-early-stage-but-investors-are-already-getting-excited/

Quantum computers have captured the imagination of scientists for many decades, and now they are coming to the attention of deep-pocketed investors, too.

According to market data analyst Pitchbook, this year has already seen $1.02 billion worth of private money funneled into the quantum computing industry -- more than the three previous years combined, even with still another few months to go in 2021.

This compares to a mere $187.5 million invested in the industry only two years ago and a total of $93.5 million all the way back in 2015.

To a large extent, this is simply due to the industry expanding. According to another analysis from consultant McKinsey, quantum computing startups have increased from a handful in 2013 to nearly 200 in 2020.

And with growth has come a clearer timeline for when quantum computers might start delivering on their extraordinary promises. Last year, IBM led the way in unveiling its roadmap for quantum computing and teased a 1,121-qubit

processor for 2023, which the company sees as a tipping point to overcome the hurdles limiting the commercialization of quantum systems.

Smaller companies have also made similar announcements. US-based startup ColdQuanta, which is building a quantum processor based on cold atoms, launched a 100-qubit processor this year, which it hopes to upgrade to 1,000 qubits in the next three years.

PsiQuantum, another US-based quantum company, has for its part committed to building a full-scale quantum computer by 2025.

Investor money isn't far behind those developments. "Quantum computing has been around since the 1980s, but over the past few years, we've come closer to both scaling the technology to a point where it can be used in real life as well as identifying initial use cases," Itzik Parnafes, general partner at Battery Ventures, tells *ZDNet*.

Quantum computers are built with qubits -- the quantum version of the bits that are currently found in any traditional computer. Qubits are capable of storing huge amounts of data, equipping quantum computers with exponential amounts of compute power that could enable them to carry out calculations that would be impossible to resolve with current machines.

The technology, say researchers, will in principle cause breakthroughs in virtually every industry, ranging from drug design to supply chain management through finance, transport and energy.

That is, in principle. Qubits are extremely difficult to manipulate. Most companies in the space are still working on building a quantum computer that actually works at a large scale, meaning that there is very little that the technology has proven so far.

Most scientists agree that a fully-fledged quantum computer is still over a decade away, but this isn't stopping companies from investigating how the technology might boost their business outcomes once it is mature enough to be commercialized.

Goldman Sachs, for example, is looking at ways that quantum algorithms could optimize the pricing of portfolio assets based on the risk that is inherent to different options, stocks, currencies and commodities. In transport, car manufacturer Daimler is exploring how quantum computers could simulate new materials to develop higher-performing, longer-lasting and less expensive car batteries.

According to Pitchbook, the field is so active that there could be some early use cases emerging in as little as three to five years, even if the technology is yet to be fully mature. This aligns with other predictions: Goldman Sachs said that quantum algorithms could start improving the outcomes of financial operations in only five years.

"While a so-called fault-tolerant universal quantum computer might be years away because we need more science to reach this point, we already have quantum computing architectures that will solve problems of interest for end-users in this time frame," Christophe Jurczak, managing partner of deep physics venture fund Quantonation, tells *ZDNet*.

"We should think about these processors as special purpose co-processors, a little bit like GPUs or AI chips in the high performance computing world. They will solve problems, not all of them but many of practical interest," he continues.

Jurczak sees those co-processors starting to play a role in fields like drug design in a couple of years, which is contributing to aggressive VC investment in the field. According to Quantonation's estimates, the total capital invested in quantum computing by the end of 2021 could reach up to $3 billion, when including announced SPACs and IPOs.

The most significant deals feature PsiQuantum, which secured a $450 million round this year to reach a valuation of $3.15 billion. IonQ, which is another contender in the race to build a useful quantum computer, is planning to go public by merging with a SPAC at a valuation of $2 billion. And startups like Zapata Computing, Quantum Machines, Rigetti and Xanadu have all raised multi-million rounds over the past couple of years.

The numbers might seem high, especially for a technology that is yet to do anything useful. Jurczak acknowledges the risk of over-hyping quantum computing, but he also stresses that the industry is at a stage where it most needs VC cash.

Since the future of quantum computing lies in the development of hardware, significant capital investments are needed – and even bigger deals are likely to be announced in the coming years.

"We need more investors and more funding, and also more projects," says Jurczak. "It is just the beginning and referring to the value creation that's expected in the long-term – up to $850 billion according to a recent report by BCG -- I think that we should not be surprised that we see such deals, especially for late-stage companies."

Last June, Battery Ventures participated in a $50 million investment in Quantum Machines, a startup that is developing a "quantum orchestration platform" that makes it easier and more practical to control quantum hardware and software.

With this investment, the VC fund is hoping to grow the wider quantum ecosystem, rather than focusing purely on quantum processors, in a move that the company describes to *ZDNet* as "taking us closer than ever to utilizing the computing potential."

But despite those encouraging prospects, Battery Ventures is keeping a cool head. "We'll have to wait for the future in order to look back and acknowledge whether quantum is currently over-hyped," Parnafes tells *ZDNet*. And as the industry grows more, it is likely to become even harder to distinguish quantum computers' promises from reality.

34. Quantum Computing Readiness: 3 Areas to Focus on Today

by Mike Brown
https://www.venafi.com/blog/quantum-readiness-3-areas-focus-today?utm_campaign=mike-brown-quantum-computing-readiness-3-areas-to-focus-on-blog&utm_medium=email&_hsmi=165004420&_hsenc=p2ANqtz-_Sh1yUce1meJ_LZ4Pa3Ql5nfoolh0S8YzxZLqu-UfyIboKWdYDeSC5w5uVtli__weX3gFFZMEJku60P-6ZbrnmOKgEXA&utm_content=165004420&utm_source=hs_email

Over the last 30 years, advancements in quantum computing have posed a challenge to the security of cryptography as we use it today. Both RSA and ECC will be broken, and symmetric key algorithms will be weakened because of this risk. As a result, governments across the world are investing billions of dollars to stay on top of these advancements. From a machine identity management perspective, the most important change is coming from the standardization of the quantum safe algorithms being carried out by NIST. This means we'll see a transition period as we work through the migration to new crypto, like we did for SHA-1, which took years to complete. But this time we have the ability to make the transition as efficient and seamless as possible.

The business impact of delaying quantum readiness will include vulnerability to breaches, reputation damage, and financial loss. And so, the question for us is what should we do about it now to minimize the potential impact? We want to be prepared. To do so, we need to take the following two steps. First, to avoid data compromise, we need to implement quantum safe crypto. Second, we want to be able to do it fast, so we need to modernize with speed and agility and be able to quickly respond and adapt to attacks while we're reducing the cost of remediation.

Are these quantum security measures achievable for machine identities? Well, we certainly need to move to quantum persistent crypto, but we also need to maintain sound machine identity management practices. And this includes visibility, automation, and policy enforcement. We need to protect all machine identities, and we need to make sure that the integrations are easy to do.

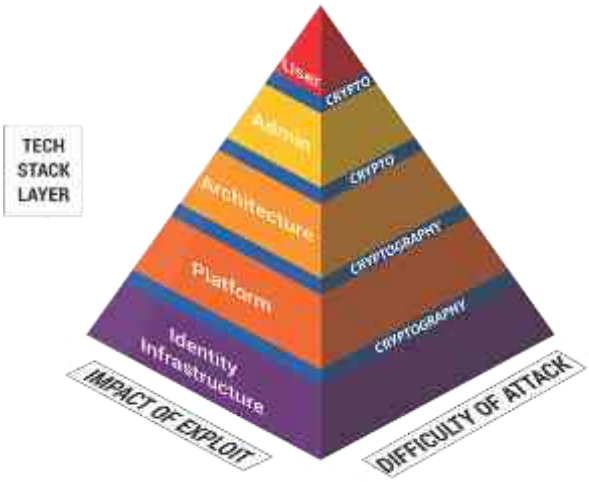
Where do we start?

There's all of this work that we're beginning to think about around how we prepare machine identities for protection against the quantum threat. Let’s start by focusing on what this means from your organization's perspective and how this starts to impact your systems. We hear about quantum impacts everywhere—including in movies and TV shows. Quantum computers are often seen as these fantastical new machines that are being developed all around the world right now. Governments and industries, from the largest enterprises to the newest startups, are focusing on quantum computing. And that's mainly because they have this promise of building and solving problems that we can't solve today.

Quantum computers are very good at one specific math problem—and that math problem unfortunately underlies the cryptography that we use to protect the internet today. Shor's algorithm is used to solve this really cool math problem. Shor’s algorithm, running on a large-scale quantum computer, makes the encryption we rely on today for our internet communications and public key infrastructure—such as RSA and Elliptic Curve — obsolete. What? No security? Now this sounds like a doomsday type scenario. Don’t despair, it's not. This is a planning problem, and we need to start by clearly understanding how big this issue is and where it affects our systems.

If we look at this pyramid, we can see that the cryptography we rely on is everywhere within our organizations. For example, you have a certificate and you use it to access your systems, but it impacts platforms and the architecture of the computer systems that you use, the ability to authorize administrative commands, even how users interact with something like online shopping.

You know these are all super important, and as an organization you need to start thinking about how we prepare our systems to be ready. This may sound like too big of a problem to solve. But it's really not. Your success will be measured in terms of planning and preparation. So, let's look at some specific use cases to help focus your efforts



(i) Future-proof your communications systems

If I'm in an organization today, and I'm thinking about preparing for the quantum threat, the first thing I'm going to do is focus on future-proofing communications. Quantum computers are expected about 10 years from now. If they can break commercial communications, then I need to ready my communications today so that they are protected 10 years from now. I should start looking at solutions now to prepare and protect my communications systems.

(ii) Plan your identity and access management migration

Even with new algorithms and processing power, machine identities will still have a strong role in protecting quantum computing. Now, I have this public key infrastructure, the Certificate Authority, that we use for protecting and identifying and authenticating users in my environment. Machine identities are impacting and being used by so many different systems in my environment. I need to start thinking about that IT migration problem and solve it to make sure my systems are ready today for quantum developments tomorrow.

(iii) Prepare for authenticated software and firmware updates

We will still need to authenticate machines in a post-quantum world. For example, my vehicle that might be getting software updates over the air is relying upon a root of trust, which I know needs to be protected in order for my software update to be authenticated. If I'm a car manufacturer, or I'm an OS provider who is relying on a root of trust within a computer system, I should start thinking today about how I protect myself from the quantum threat so that my over-the-air software updates can't be spoofed by an adversary.

As you can see, if you have not started already, it's time to get planning! At ISARA, we have been working to bring the tools and the knowledge needed to face new quantum risks. This summer, we announced a cryptographic management platform that reveals your blind spots and most importantly, equips you to take action. Additionally, we have collaborated with Venafi and Crypto4A through the Machine Identity Management Development Fund to build integrations with the Venafi Trust Protection Platform to enable a quantum-safe solution that you can start using today.

35. Cambridge Quantum Scientists Release Two Studies Focusing The Power of Quantum Computing to Solve Real-World Problems

by Matt Swayne
https://thequantumdaily.com/2021/09/15/cambridge-quantum-scientists-release-two-studies-focusing-the-power-of-quantum-computing-to-solve-real-world-problems/

Cambridge Quantum continues to drive research toward bringing quantum computers into mainstream usage, this time publishing two studies aimed at allowing quantum computers in their current stage to solve difficult problems and complex calculations.

In a statement on LinkedIn, the company reports the papers were published arXiv, a pre-print server. One study is on Quantum Monte Carlo integration (QMCI) and the other is on Quantum Amplitude Estimation (QAE).

According to the company, the research represents important steps to bring about practical quantum computing.

The researchers said the QAE study that quantum algorithms can still work well in the presence of noise, an important concern in the Noisy Intermediate-Scale Quantum — or NISQ — era.

They write: "CQ shows that when the algorithms in question are sampling-estimation algorithms then the answer is an emphatic 'yes' — in fact, in classical signal processing, they have been doing exactly this for decades. We show that QAE is an ideal candidate for this approach by using the structure of the quantum circuits used in QAE to derive a bespoke noise model, which is then used to extend the range of QAE when performed on NISQ devices."

This team includes Steven Herbert, a senior research scientist; Roland Guichard, research software developer and Darren Ng, all of Cambridge Quantum.

To confirm the validity of the approach, the researchers ran their experiments on IBM and Honeywell's quantum computers.

The work fills two significant gaps, and the two papers represent an important step towards being able to apply QMCI to real-world problems.

"We have further shown how our proposed noise model can be used to inform the design of, and improve the parameter estimation in, QAE – yielding a first proposal for how to achieve noise aware QAE," the team concludes.

The second paper, which complements the QAE study, introduces Q-marginals and demonstrates the construction of a quantum sampling circuit from its classical counterpart. Q-marginals are quantum states encoding some probability distribution in a way that can be used in Quantum Monte Carlo Integration (QMCI), an approach that numerically

estimates the mean of a probability distribution by averaging sample and could be used to help financial researchers manage risk and pharmaceutical firms find drugs for disease

Herbert, author of the study, explains that the work is important because quantum advantage in Monte Carlo integration is in the form of a reduction in the number of uses of a quantum state encoding the probability distribution (in QMCI) relative to the number of samples that would be required in classical MCI. Therefore, it only translates into a computational advantage if the number of operations required to prepare this quantum state encoding the probability distribution is comparable to the number of operations required to generate a classical sample.

Cambridge Quantum and Honeywell recently announced a merger, uniting two quantum research powerhouses.

36. Quantum cryptography: This air-filled fiber optic cable can transport un-hackable keys, say researchers

by Daphne Leprince-Ringuet
https://www.zdnet.com/article/quantum-cryptography-this-air-filled-fiber-optic-cable-can-transport-un-hackable-keys-say-researchers/

A new type of optical fiber filled with nothing but thin air has been found to be particularly effective for carrying out quantum key distribution (QKD), a security protocol that is in principle un-hackable and could play a key role in protecting sensitive data against ever-more sophisticated cyberattacks.

BT experimented with QKD over a six-kilometer-long cable of hollow core fiber, a technology that it has been working on for the past few months as an alternative to traditional fiber optic cables.

Optical fiber is typically made of solid strands of glass that carry information by channeling light signals emitted by laser transmitters. Hollow core fiber, on the other hand, has a hollow center filled with air, which runs the entire length of the cable and is encased in a ring of glass.

It turns out that this configuration is better suited to QKD, because it reduces the possibility that different signals interfere with each other and spoil the whole process.

QKD works in a similar way to traditional cryptography: data is encoded into an unreadable message thanks to a cryptography key that the recipient needs to decrypt the information. The method works by encoding the cryptography key onto a quantum particle (or qubit) that is sent to the other person, who measures the qubit in order to obtain the key value.

This approach is particularly interesting to security researchers because it is based on the laws of quantum physics, which dictate that qubits collapse as soon as they are measured. This means that if a third-party eavesdrops on the exchange and measures the qubits to figure out the cryptography key, they would inevitably leave behind a sign that they have intruded.

Cryptographers, therefore, call QKD "provably" secure. The method is expected to bring an additional level of safety to data exchanges, especially as hackers develop better tools to crack existing security protocols.

The technology is nascent, and researchers are looking at various ways to carry out QKD; but one of the most established approaches consists of using optic-fiber cables to send both the qubits that are loaded with the cryptography key, and the actual encrypted message.

But when using traditional optical fiber, which is made of glass, the effectiveness of the protocol is limited. This is because the light signals that carry information are likely to spread their wavelengths when travelling through glass, an effect called "crosstalk" that causes channels of light to leak into other channels.

For this reason, the encrypted message cannot be sent through the same cable as the qubits, which are exceptionally fragile and susceptible to the noise caused by crosstalk. The whole process, says BT, is comparable to trying to have a whispered conversation next to an orchestra.

This is where hollow core fiber could make a big difference. In an air-filled channel, light signals don't scatter as much, and less crosstalk occurs between channels. In other words, there can be a clear separation between the encrypted data stream and the faint quantum signal that carries the encryption key – even if they are both travelling over the same fiber.

Ultimately, therefore, hollow core fiber could be a more efficient candidate for QKD – an "all-in-one" solution that requires less infrastructure to be built.

"We know now that if we were to put hollow core fiber in, it could enable us to put quantum channels potentially anywhere we like, without having to worry," Catherine White, a researcher at BT, tells ZDNet. "Whereas with standard fiber, we either have to assign separate fibers for the QKD system or we have to be really careful not to have too much on classical power when doing the planning."

What's more, in previous trials of the technology, BT has also demonstrated that sending light signals through an air-filled core is much faster than through glass: according to the company, hollow core fiber enables data to travel up to 50% faster than in traditional optical cables.

This means that the technology could also significantly reduce latency in the transmission of data. "This trial shows us the material we can work with, and it has wonderful properties like low latency and low scattering," says White.

BT's trial remains limited: the experiment didn't go so far as exchanging actual encrypted data, and instead looked at the behavior of the quantum particle when it was sent alongside a high-power classical channel, in this case a light signal. The success of the trial, says White, lies in the fact that both channels remained healthy, which wouldn't be the case with standard fiber.

"We were just proving key exchange, not testing encryption in this case," says White.

But parameters from the trial, such as quantum bit error rate, indicate that the system effectively generated a key that could be used to protect data, continued the researcher. Experiments are now underway to apply the configuration to the exchange of data.

The next challenge will be to find out whether the technology can be scaled up. BT trialed QKD on a six-kilometer-long cable – still far off other experiments with the protocol in which researchers have managed to deliver quantum particles over hundreds of kilometers.

Earlier this year, for example, researchers from Toshiba Europe's Cambridge Research Laboratory demonstrated QKD on optical fibers exceeding 600 kilometers in length.

White explains that, for all its low-latency and low-scattering properties, the hollow core fiber used in BT's trial is not low-loss, which is a crucial property to extend the reach of QKD. Researchers, however, are working on fine-tuning the material to improve its performance in that respect.

"Findings show that, when tuning the fiber for particular wavelengths, we are able to have astoundingly low loss," says White. "This is very promising and we will see further developments. It does mean that hollow core fiber could potentially help reach longer reaches of QKD than we've seen."

37. Cryptographic Catastrophe Theory

by John Levine
https://circleid.com/posts/20210914-cryptographic-catastrophe-theory

Technologists and law enforcement have been arguing about cryptography policy for about 30 years now. People talk past each other, with each side concluding the other side are unreasonable jerks because of some fundamental incompatible assumptions between two conceptual worlds in collision.

In the physical world, bank branches have marble columns and granite counters and mahogany woodwork to show the world that they are rich and stable. This works because that kind of building is slow and expensive to construct. Even if something with marble and mahogany is not exactly a bank, it is still likely to be rich, stable, and bank-like. But on the Internet, whatever a bank can do on their website, bored teenagers in Moldova can copy, which is one of the reasons we have so much phishing. People's assumptions about what banks look like not only fail, but they don't fail a little bit; they fail catastrophically.

In the physical world, when things fail, they tend to fail gradually. It is not surprising when a building has leaks and cracks, but very surprising when it collapses. Pre-computer security models generally failed a little bit, too. If the law says you need a court order for a wiretap, and someone lies to a judge or sends the phone company a forged order, that lets them tap one line, not the entire phone system.

But in software, catastrophic failure is normal. Software security breaches don't just disclose one or two account credentials; they leak every user's credentials. They don't give the attackers access to one customer's network; they get into every customer's network.

Cryptographic software has the same problems as any other software. Decades of effort have told us that cryptographic software can fail and if it fails, it is likely to fail catastrophically.

This is where the talking past each other happens. Law enforcement people who want back doors or lawful access or whatever it's called these days, have a wiretap mental model. There are rules to control who gets to use the back door. They will mostly work, and the costs when they don't are contained. So it's a small decrease in security, a reasonable tradeoff to fight all that crime.

We, software people, have the catastrophe model. If you build a back door into your device, the system will always be one disaffected clerk or one misconfigured server away from hostile private and state actors being able to open that back door anywhere, any time, a catastrophic failure. Personally, I think that's a much more likely scenario.

It's not like we haven't tried to explain this, but the people who believe in the wiretap model believe in it very strongly, leading them to tell us to nerd harder until we make it work their way, which of course we cannot.

I don't see any way out of this impasse, which does not mean I am ignoring or minimizing the issues that law enforcement is trying to deal with. But compromise with catastrophe just doesn't exist.

38. Crypta Labs Develops World's First Space Compliant Quantum Random Number Generator For UKRI & The UK Space Agency

by James Dargan
https://thequantumdaily.com/2021/09/14/crypta-labs-develops-worlds-first-space-compliant-quantum-random-number-generator-for-ukri-the-uk-space-agency/

Crypta Labs has completed the Space Research and Innovation Network for Technology (SPRINT) project to develop a Quantum Random Number Generator for space which will facilitate quantum secure encryption of satellite data

Crypta Labs is proud to announce the successful conclusion of our Quantum Random Number Generator (QRNG) for use in the Low Earth Orbit environment project, conducted alongside the University of Southampton as part of the Space Research and Innovation Network for Technology (SPRINT), funded by the UK Space Agency and UKRI.

The Crypta Labs QRNG devices were tested by the University of Southampton in a thermal vacuum, cycling between temperatures of -50C and +80C, during which the team in Southampton were able to generate high-quality random numbers at a bitrate of 40 Mbit/s. The devices were then subjected to vibration tests simulating the launch environment of a Soyuz and Falcon 9 vehicles—all devices successfully completed the tests and came out fully operational.

Jean Paul Ludig, Crypta Labs head of operations said: "We are grateful to the SPRINT programme and the fantastic team at Southampton University for allowing us to prove that our patented QRNG can withstand extreme environmental conditions robust enough for space. Hopefully, this will encourage dialogues with defence and aerospace vendors looking to integrate quality quantum random numbers to provide the next constellations of Quantum Satellite Communications. This is a huge milestone in achieving our vision to accelerate the adoption of Quantum technology."

Charlie Ryan, lecturer in astronautics at the University of Southampton added: "It has been great to work with such a dynamic company on a very innovative product. It has allowed us to increase our experience of verification testing of spacecraft components, and we look forward to working with Crypta Labs again in the near future."

Martine Harvey, interim head of SPRINT programme said: "SPRINT has already engaged with more than 450 businesses across the UK, enabling more than 90 collaborative innovation projects across the UK. One of our primary aims is to enable businesses to develop new cutting-edge space technologies so we're delighted that Crypta Labs has successfully completed its project in collaboration with the University of Southampton."

Crypta Labs is a London-based quantum security company with the vision to provide more secure connections to connected devices. We aim to accelerate the adoption of Quantum Random Number Generator technology as a key component of cyber security to help mitigate this threat and make the world a safer place.

The University of Southampton is a member of the Russell Group of universities, with a research-led approach to the education of its students of which there are currently about 23,000. It has a particularly strong national and international reputation in engineering with one of the largest engineering faculties in the country.

The Faculty of Engineering Physical Sciences contains the Department of Aeronautics and Astronautics, which is celebrating its 60th anniversary in 2019, being the second oldest department with such a name in the world.

The Department is one of the most established aerospace engineering research centres in the UK, with specialisms including autonomous vehicles, complex fluid phenomena, and spacecraft engineering.

SPRINT is the Space Research and Innovation Network for Technology, a unique partnership of top UK space universities, industry, government agencies and the investment community dedicated to supporting the growth of small to medium enterprises (SMEs) in the UK through the commercial exploitation of space data and technologies.

39. China's Origin Quantum Sets Roadmap, Sees 1,024-Qubit Device by 2025

by Matt Swayne
https://thequantumdaily.com/2021/09/14/chinas-origin-quantum-sets-roadmap-sees-1024-qubit-device-by-2025/

As a gift for it fourth anniversary of its founding, China's **Origin Quantum** set an ambitious roadmap with the development of a 1024-qubit quantum computer by 2025, according to computer-translated company statement.

The announcement said that the roadmap predicts the company would launch a 64-bit superconducting quantum chip by the end of 2021 and further improvements would continue in three stages over the next few years. Origin is a leading quantum computing company located in China's Hefei High-tech Zone.

"The new design layout increases the scalability of the chip," the company said. "At the beginning of 2022, it will try to break through 144 bits. By 2025, 1024 qubits will be realized."

Zhang Hui, general manager of Origin Quantum, said that the first stage includes work on a superconducting quantum computer prototype before 2022, focusing mainly on chip fidelity and scalability. The second phase will break through to 1000 qubits in 2025 and try to solve special problems in various industries and develop industry fields. In the third stage, multi-core parallel processing is used as the number of chip bits reaches a certain level.

"The quantum computer operating system independently developed by the source can realize full scheduling of quantum resources and is expected to realize a general-purpose quantum computer," the company reports.

Zhang Hui said that current research and development is moving from quantum computer prototypes to NISQ quantum computers.

The 1000-plus qubit goal is shared by other quantum computer makers, including IBM. Origin calls the 1000-plus goal as a "key node "for the expansion of general-purpose quantum computers. But it's really just the beginning, Zhang Hui said.

"Once the quantum computer of the superconducting physics system reaches 1000-plus qubits, it may be a devastating blow to other technological paths." Zhang Hui said. "But for general-purpose quantum computers, it may still need to reach a million bits. At present, one of the biggest problems to be overcome in the realization of a general-purpose quantum computer is to solve the problem of error correction and fault tolerance. If the problem of error correction and fault tolerance cannot be solved, it may not be possible to realize a general-purpose quantum computer for a long time. It has no effect on special quantum computers. But if it is like the classical computers we are using now, it is error-correcting and fault-tolerant. Once a breakthrough is made, general-purpose quantum computers will be just around the corner."

Underlying the roadmap is Origin's desire to move the quantum computer out of lab and into people's lives. To do that, the company has connected with other industries that will one day use quantum computers to solve difficult problems.

Origin Quantum established China's first quantum computing industry alliance. They added that many domestic companies have joined the Quantum Industry Application Alliance, including CCB International, Orient Securities, CICC Capital, UnionPay Commerce, Demei Chemicals, GenScript, Hanhai Boxing, and Ruikang Biotechnology.

Zhang Hui said, "But it is already obvious that quantum computing has the potential and ability to change the entire economy and society. And when the research and development of the original quantum breaks through 1,000 qubits, these industries will also undergo tremendous changes. Our original What quantum can do is to hold on to this track firmly, so that China will not be controlled by others in the field of quantum computing."Origin Quantum was established on September 11, 2017. It is the first quantum computing company in China to officially promote quantum computing to the commercial field. It is a.The company's technology is traces back to the Key Laboratory of Quantum Information of the Chinese Academy of Sciences, combined with the quantum chip super 973 project undertaken by Professor Guo Guoping's team over ten years.

40. BT Conducts Trial of Quantum-Secure Communications Over Hollow Core Fibre Cable

by Matt Swayne
https://thequantumdaily.com/2021/09/13/bt-conducts-trial-of-quantum-secure-communications-over-hollow-core-fibre-cable/

BT announced that it has achieved a new milestone in the development of quantum-secure communications by conducting the world's first trial of Quantum Key Distribution (QKD), a method of ultra-secure communications, over hollow core fibre cable, from Southampton University spin out, Lumenisity® Limited.

This summer, BT kicked off trials of a new type of optical fibre – Nested Anti-Resonant Nodeless Fibre (NANF) hollow core fibre – at the BT Labs in Ipswich to test the potential benefits of deploying this technology for a variety of scenarios, including secure communications. The trials used cable developed and manufactured by Lumenisity to address the need for high-speed transactions and bandwidth increases in advanced communications systems, which has also been used for applications such as Data Centre Interconnects (DCIs), Edge and 5G xHaul.

In the latest trial, BT researchers successfully operated a state-of-the-art QKD system using commercial equipment over a 6-kilometre-long Lumenisity CoreSmart® cable with a hollow, air-filled centre, revealing potential benefits such as reduced latency and no appreciable crosstalk – the effect of a transmitted signal interfering with the transmission of another signal.

In most optical fibre communications, high-speed signals are sent over a solid piece of glass using different wavelengths of light to deliver high capacity transmissions. In QKD systems, quantum light is transmitted on a single photon channel, traditionally necessitating use of a separate fibre, due to 'crosstalk 'an effect that causes the light from high-speed data channels to spread their wavelengths, interfering with a quantum signal carried over the same fibre, as the change in frequency can cause channels of light to leak into other channels. The effect is similar to having a whispered conversation next to an orchestra – it can be hard to hear the other person's voice over the music.

Hollow core fibre doesn't have internal material – it's filled with only air – so there is less light scattering and less crosstalk between channels, even at a single photon level. This clearer separation – similar to a wall between the two speakers and the orchestra – makes it easier to deliver both a high-speed encrypted data stream, and the faint quantum signal that carries the encryption key, over the same fibre.

Lumenisity's cable also demonstrated further benefits for the deployment of QKD, as commercial telecommunications equipment will not need to be optimised in order to send a data-encrypted key. This is critically important because the equipment can be used normally without modifications, an issue that creates added complications for sending secure signals over standard fibre.

Professor Andrew Lord, BT's Head of Optical Network Research, said: "This is an exciting milestone for BT, accelerating the UK's lead in quantum technologies that will play an important role in future communications systems globally. We've proven a range of benefits that can be realised by deploying hollow core fibre for quantum-secure communication. Hollow core fibre's low latency and ability to send QKD over a single fibre with other signals is a critical advancement for the future of secure communications."

Tony Pearson, VP Sales and Marketing at Lumenisity, said: "We are excited to be identifying new applications for our field deployable CoreSmart cable solutions and working with the BT team on the first trial in the world of this kind. This milestone further accentuates not just the capability of our hollow core cable solutions, offering low latency and high bandwidth, but also demonstrating the potential CoreSmart has in new applications thanks to ultra low non-linearity and dispersion across a broad spectrum, perfect for networks operated by our Carrier partners."

41. Error-Correction, A Bridge or a Bandage in the NISQ Era?

by Matt Swayne
https://thequantumdaily.com/2021/09/13/quantum-insider-insights-error-correction-a-bridge-or-a-bandage-in-the-nisq-era/

The pace of exciting research in error-correction has quickened for both university and corporate research groups. Some experts believe that error-correction will create quantum advantage — a point at which quantum computers can outperform classical computers at some tasks — much quicker than originally thought. Others suggest that these techniques will have to work because fault-tolerant quantum computers are still years (at least) away.

In this Quantum Insider Insights, we'll take a look at some of this research, review research on just how necessary this error correction is — and analyze the debate on the role error-correction will play in getting us to the quantum era.

42. Is quantum-as-a-service about to go mainstream?

by KEVIN POIREAULT
https://sifted.eu/articles/quantum-service-oqc/

This summer Oxford Quantum Circuits became the latest quantum computing company to make their quantum hardware available to users over the cloud — the first UK company to offer quantum-as-a-service.

The Reading-based startup is joining the ranks of the big Silicon Valley tech companies Google, Amazon and IBM in offering QCaaS. While its system can't quite compete with the number of qubits that these big challengers have to offer, it is a sign of how quantum computing is coming into the mainstream.

Let's be clear — quantum computers aren't terribly useful right now. Despite a few lab demonstrations of quantum supremacy — where quantum computers perform a function better than a classical supercomputer — in the real world companies are still struggling to find a compelling use case.

Companies like OQC are hoping that their quantum-as-a-service offerings will change that.

The pressure is on

Quantum computing companies are coming under pressure to prove their worth. Over the past year, we've seen a quantum frenzy.

Investment is at an all-time high: overall investing in the sector has reached $2.5bn so far this year, up from $1.5bn in all of 2020 and less than $500m each of the previous year, according to financial data firm PitchBook.

But much of the quantum computing capability remains severely underpowered. OQC's quantum computer, which is based on superconducting qubits, cooled down a temperature close to absolute zero, has only 4 qubits, compared with the 65 that IBM's Hummingbird can give you access to.

However, OCQ's CEO Ilana Wisby argues that the high quality of the qubits at least in part compensates for that: "With this 3D proprietary qubit architecture invented by OQC's founder Peter Leek at the University of Oxford, called the Coaxmon, we have demonstrated incredible coherence and incredibly low cross-talk by taking all of the control wiring that usually networks the qubits on the same plane."

Some remain sceptical about this. Olivier Ezratty, a French consultant and author of Comprendre l'informatique quantique (an English version is to be published in September) points out that OQC's press release "didn't come with a scientific paper on their hardware product nor did they give any more detail about the QCaaS offering".

It is a tendency that Ezratty has seen a lot lately. "Since the beginning of the year, more and more startups are jumping on the quantum bandwagon yet they have in their hands a piece of hardware that is not ready to compete with what is on the market".

Ilana Wisby evades this issue but instead elaborates on the encouraging results that OQC's first client, Cambridge Quantum (CQ) has been able to show with its IronBridge cybersecurity platform. "We ran 5,000 programmes per second with a total of 10 million programmes execution", she claims. "The results of the application will be published as part of a wider publication by Cambridge Quantum."

Wisby also told Sifted that OQC was working on a next deployment with many more qubits, that they will soon make public.

43. Is your organization prepared for the arrival of quantum computing?

by Tim Callan
https://www.securityinfowatch.com/cybersecurity/information-security/managed-network-security/article/21237601/is-your-organization-prepared-for-the-arrival-of-quantum-computing?utm_medium=email&_hsmi=165004420&_hsenc=p2ANqtz-9Wy2Acjri1JjgTM3_GmThMZjX3ROd_I1SeEZJb1Sb1Mdxdlsic36ZJN9NnaMhbiH3DNZnyIFx9XA-iDQ9aD_WSSvn4MQ&utm_content=165004420&utm_source=hs_email

The arrival of quantum computing will cause a ripple effect that will touch every corner of the technological landscape. This isn't an exaggeration—it's a fact. In general terms, quantum computers will be able to solve certain complex problems much more quickly than traditional computers are able to today. In more specific—and concerning—terms, quantum computers will be able to crack much of today's most widely used cryptographic algorithms. It isn't hard to

imagine the catastrophic consequences of this veritable cryptographic skeleton key falling into the wrong hands. Preventing this disaster will necessitate a complete overhaul of the way organizations approach encryption.

Practical quantum computing has not yet arrived, but steady progress has been made by companies like Google, Microsoft, and others vying for what many have dubbed "quantum supremacy." Make no mistake: quantum computers are on the way, and they will be here sooner rather than later. Preparing for the cryptographic apocalypse should be a top priority for today's IT teams. Any organization failing to plan for the inevitable shift to new quantum-resistant algorithms risks falling dangerously behind, leaving their network and devices exposed to savvy attackers ready to exploit those who fail to adapt to the new reality.

Understanding the Cryptographic Quantum Apocalypse

In 1994, a mathematician by the name of Peter Shor discovered a new algorithm capable of breaking conventional public-key cryptography—but it required a then-theoretical quantum computer with a certain number of qubits (a basic unit of quantum information). Shor's algorithm, as it would come to be known, demonstrated that a quantum computer can factor integers much more efficiently than a traditional computer. Unfortunately, this would make quantum computers much more efficient at cracking Rivest-Shamir-Adleman (RSA) encryption and elliptic-curve cryptography (ECC)—the two most common types of encryption in use today.

IT professionals know how essential encryption is to every facet of modern life, but it is worth taking a moment to stress the sheer number of industries and critical processes it touches. Encryption has fundamental uses in government, defense, finance, commerce, communication, transportation, healthcare, and logistics, to name just a few. The systems using encryption (public key infrastructure, or PKI) help secure everything from email accounts and Internet of Things (IoT) devices to financial transactions and healthcare data. In short, the arrival of quantum computing will effectively force nearly every organization on the planet to rethink its approach to encryption before it's too late.

Making the Most of a Head Start

The coming cryptographic quantum apocalypse is neither a secret nor a surprise. Security and IT professionals have known this was coming for some time. In fact, one could argue they have known this was a likely possibility since the discovery of Shor's algorithm, but recent progress in the field of quantum computing has suddenly made it a much more tangible threat.

The arrival of quantum computing began to feel more imminent in 2019 when the public at large—and not just specific mathematicians—began to realize the impending need for new cryptographic algorithms. Throughout 2020, a considerable amount of work was done, both by those working to develop quantum computers and those working to defend against their capabilities. Quantum computers are consistently growing more powerful, with an increasing number of stable qubits. The development will likely continue at this steady pace—it seems unlikely that there will be a "eureka" moment in the immediate future, where the number of stable qubits suddenly begins to grow at a faster rate than expected.

In many ways, this is good. Stable quantum computing will introduce exciting new technological possibilities. Its ability to solve complex problems quickly promises potential breakthroughs in fields like artificial intelligence, financial modeling, chemistry, and others. But the world is not yet prepared for the potential danger the technology brings with it. Fortunately, the National Institute for Standards and Technology (NIST) has been hard at work identifying potential algorithms capable of withstanding the expected encryption-cracking capabilities of quantum computers. The organization has been soliciting quantum-resistant encryption algorithms since 2015 and has since narrowed the 69 candidate algorithms it received down to the nine most likely to lead to viable, quantum-safe encryption methods.

Though there is no firm timetable, NIST plans to release its final list of recommended algorithms sometime in the near future.

Quantum Skepticism Has Risen, but Don't Be Fooled

Not every organization is ready to upend its operations to account for quantum computing, and IT and security professionals have noticed even some computer scientists expressing skepticism over whether quantum computing will live up to its considerable hype. This is understandable—for a long time, quantum computing was the quintessential technology that was perpetual "five years away," always coming "soon" but never seeming to get any closer. With that in mind, it isn't hard to see why some technology experts are challenging the idea that the world is on the verge of a quantum computing breakthrough—or even that it will have as great an impact as people fear.

While understandable, this skepticism is dangerous. Ready or not, quantum computing is coming, and every form of encryption in widespread use today is vulnerable to Shor's algorithm. Short of quantum computing development stopping dead in its tracks, quantum computing will inevitably defeat conventional cryptography. Anyone using any form of encryption needs to be prepared to replace it with a quantum-safe alternative.

One might even argue it is too late. Cybercriminals who believe in the viability of quantum computing may already be planning for a post-quantum future: after all, if an attacker has harvested and stored an encrypted file, all it needs is a quantum computer to crack it. Today's attackers have demonstrated a clear willingness to play the long game, laying the groundwork for attacks months (even years) before their execution. Attackers are not taking a "wait and see" approach to quantum computing—they understand that if they can get their hands on encrypted files now, it is just a matter of time until they have the ability to crack them. Today's organizations should assume any information they transmit could be recorded by malicious parties waiting for the chance to decrypt it.

Who Needs to Hear This?

Given the critical role encryption plays in modern society, it is not an exaggeration to say that any organization sending or receiving information encrypted with a traditional algorithm needs to be planning for a post-quantum future right now. This applies to any organization using email, file transfers, financial transactions, cloud storage, SSL certificates, and countless other modern conveniences. In other words, just about everyone.

IoT device manufacturers stand out as particularly vulnerable. Consumer IoT devices have an average lifespan of three to five years, while commercial devices tend to remain in use for seven to 10 years—meaning manufacturers need to plan for the long term. Manufacturers absolutely need to begin wrapping their heads around quantum cryptography and putting a plan into place regarding how to implement it once the algorithms are finalized. This has admittedly put manufacturers in a sticky situation: some may need to decide whether to delay a product until after NIST makes its final recommendations. For some companies, a product delay may not be financially viable, but releasing a potentially vulnerable product can put the company in an equally dangerous predicament.

When it comes to the cryptographic quantum apocalypse, planning ahead is the only way to survive. Organizations need to take advantage of the head start they have been given. In addition, even without the final algorithms, manufacturers can begin planning firmware updates designed to implement quantum-safe encryption. Failure to do so may force a company to later recall or replace devices that cannot be updated sufficiently. It is imperative for decision-makers ranging from those dealing with cryptography and digital certificates to those issuing company laptops to begin educating themselves on quantum cryptography.

The Time to Act Is Now

Updating all encryption across an entire organization cannot be done with the snap of a finger. It takes time. But an organization starting the process now might be finished in a year—well before potential attackers will be in a position to exploit the power of quantum computing. On the other hand, an organization waiting to act until NIST finalizes its list of algorithms (or IBM or Google announces the creation of a quantum computer capable of breaking RSA encryption) will be scrambling to play catch up.

The time to act is now. Organizations need to begin conversations with board members and C-Level executives to impress upon them the urgent need for those changes. The need for quantum-safe cryptography has been apparent for years, and some of the smartest people in the world have been working on it. But organizations must *choose* to act—and those that don't may quickly find it is too late to catch up.

44. The Post-Quantum Cryptography World is Coming: Here's How to Prepare

by Jennifer Gregory
https://securityintelligence.com/articles/post-quantum-cryptography-how-to-prepare/

Have you ever sat in traffic and cursed the town planners? For years, you may have watched as the town approved new subdivisions and stores along the roads you drive often. And you wondered when they would add a new lane, extend a road or install a new stoplight. But think about this: If you're skipping over news articles about quantum computing and post-quantum cryptography, you're doing the same thing in relation to your business that town planners seem to do relative to new construction — waiting for the negative impacts before fixing the issue.

Much (if not most) of the time, these changes only happen after negative impacts come in force. People will go to council meetings over accidents and stop-and-go traffic. Have you ever wondered why town planners don't proactively improve the roads before the new construction is finished? I've never understood why they wait.

But instead of clogged roads, your business or agency is more likely to face data breaches and cyberattacks. In turn, these can cause financial loss, reputation damage and business disruption.

For decades, the tech industry has held up encryption as the key to keeping your data secure. With more companies changing the way they work in the pandemic, data security has become even more important. Not only do we have more transactions performed online now, but a wider range of tasks are also now online.

Quantum Computing: A Different Algorithm

At the same time the volume and type of data increased online, researchers have been focusing on developing and perfecting quantum computing. It's widely known that quantum computing is faster and can handle higher volumes than computational computing. However, not everyone knows why that's true, or why it matters for post-quantum cryptography.

It's because the algorithm takes a totally different approach. Instead of computing only with the traditional bit of a 1 or 0, quantum computing uses quantum bits, or qubits, which can also include superposition of 0 or 1. This increases the number of computations performed in the same amount of time.

Because quantum computers are out of the budget for most companies, and likely always will be, IBM and others developed a range of tools and systems that allow them to develop applications in the quantum environment without having to purchase cost-prohibitive hardware. The goal is frictionless quantum computing with developers using advanced hardware with a cloud-based application programming interface, working seamlessly with high-performance computing resources.

Developing Post-Quantum Cryptography

Making quantum computing accessible and feasible opens many doors, especially in the fields of health and science. People will be able to solve problems they never could before. However, attackers will have access to quantum computing as well. This means they will be able to use it for harm. This is Q-Day, or the moment in which quantum computing will render any of today's encryption methods, including those that protect systems like financial markets and public infrastructure, obsolete.

Using quantum computing, attackers can likely break even the most advanced encryption methods. The greatest concerns are Shor's Algorithm and Grover's Algorithm, which are two of the most touted capabilities of quantum computing. Once these are easy for attackers to obtain, they will be able to use these algorithms to break existing symmetric, and asymmetric, defenses. This means that in a post-quantum cryptography world encryption protected with RSA or elliptic-curve cryptography (ECC) can easily be cracked, opening up sensitive data to breaches and attacks.

The issue is so critical that the National Institute of Standards and Technology launched a post-quantum cryptography project to address this specific issue. The NIST started with 82 candidates for post-quantum cryptography algorithms and recently announced at the IBM cryptography meeting that it hopes to have a small number selected for standardization at the beginning of 2022. The goal is to have a final version finished around 2024.

Living in a Post-Quantum Cryptography World

Because encryption is everywhere — affecting every device, browser and application — updating encryption algorithms to be quantum-proof is a huge task. Writers often liken it to fixing the Y2K bug. And that's accurate. Once the solution exists, organizations will need to update their encryptions in everything they've developed. Every person and business must ensure that all the devices and applications they use are updated.

Now is the time to be doing what we all wish town planners would do. Once the algorithm comes out, you likely won't have much time. After all, the threat actors will have access to it, too.

Start making notes of all the areas where the systems and applications you develop use encryption. And keep a close eye on the changes happening in quantum computing.

You can then be ready to spring into action — and know exactly what to do — when post-quantum cryptography technology starts to affect you. Instead of dealing with accidents and traffic jams, your customers and employees will be driving down the road smoothly with their encrypted data well protected.

45. IonQ and University of Maryland plan Q-Lab for hands-on quantum computing research

by Veronica Combs
https://www.techrepublic.com/index.php/article/ionq-and-university-of-maryland-plan-q-lab-for-hands-on-quantum-computing-research/

IonQ is honoring its research roots by establishing a new quantum computing lab at the University of Maryland, College Park. National Quantum Lab at Maryland (Q-Lab) will be the first facility in the U.S. where scientists will have hands-on access to a commercial-grade quantum computer, according to the university. The university is making a $20 million investment to open the lab.

University of Maryland President Darryll J. Pines said in a press release that the university is excited to establish this strategic partnership and to "further solidify UMD and the surrounding region as the Quantum Capital of the world."

"No other university in the United States is able to provide students and researchers this level of hands-on contact with commercial-grade quantum computing technology," he said.

The lab is part of the university's $300 million investment in quantum science, which includes more than 200 researchers studying the subject and seven centers, including the new Quantum Leap Challenge Institute for Robust Quantum Simulation. The National Science Foundation awarded $25 million to the university this month to launch the center. Researchers will develop theoretical concepts, design innovative hardware and provide education and training for new simulation devices that can predict and understand quantum phenomena.

The lab will be in the UMD Discovery District, next to IonQ's headquarters in College Park. The university expects the Q-Lab to "democratize access to this innovative technology, generate new intellectual property and attract global scientific and engineering talent." It will join the existing Quantum Startup Foundry and the Mid-Atlantic Quantum Alliance as "another incentive for entrepreneurs and startups to bring their businesses to College Park" and add to the area's private sector ecosystem, according to the university.

Chris Monroe and Jungsang Kim founded IonQ in 2015 with $2 million in seed funding from New Enterprise Associates and a license to core technology from the University of Maryland and Duke University. Kim and Monroe wanted to take trapped ion quantum computing out of the lab and onto the market. The company plans to develop modular quantum computers small enough to be networked together by 2023.

Instead of going the IPO route as many new companies do, IonQ is merging with dMY Technology Group III, a special-purpose acquisition company. The deal includes a PIPE investment from Fidelity Management & Research Company LLC, Silver Lake, Breakthrough Energy Ventures, MSD Partners, L.P., Hyundai Motor Company and Kia Corporation.

There are more than 40,000 students,10,000 faculty and staff, and 300 academic programs at the University of Maryland, College Park. Faculty members include two Nobel laureates, four Pulitzer Prize winners and 59 members of the

national academies. The institution has a $2.2 billion operating budget and secures more than $1 billion annually in research funding together with the University of Maryland, Baltimore.

46. UTSA professor helps make break-through achievement in quantum computing

by Bruce Forey
https://www.utsa.edu/today/2021/09/story/sutherland-tyler-quantum-computing-breakthrough.html

A UTSA researcher is part of a collaboration that has set a world record for innovation in quantum computing. The accomplishment comes from **R. Tyler Sutherland**, an assistant professor in the College of Sciences 'Department of Physics and Astronomy and the College of Engineering and Integrated Design's Department of Electrical Engineering, who developed the theory behind the record-setting experiment.

Sutherland and his team set the world record for the most accurate entangling gate ever demonstrated *without lasers*.

According to Sutherland, an entangling gate takes two qubits (quantum bits) and creates an operation on the secondary qubit that is conditioned on the state of the first qubit.

"For example, if the state of qubit A is 0, an entangling gate doesn't do anything to qubit B, but if the state of qubit A is 1, then the gate flips the state of qubit B from 0 to 1 or 1 to 0," he said. "The name comes from the fact that this can generate a quantum mechanical property called 'entanglement 'between the qubits."

Sutherland adds that making the entangling gates in your quantum computer "laser-free" enables more cost-effective and easier to use quantum computers. He says the price of an integrated circuit that performs a laser-free gate is negligible compared to the tens of thousands of dollars it costs for a laser that does the same thing.

"Laser-free gate methods do not have the drawbacks of photon scattering, energy, cost and calibration that are typically associated with using lasers," Sutherland explained. "This alternative gate method matches the accuracy of lasers by instead using microwaves, which are less expensive and easier to calibrate."

This quantum computing accomplishment is detailed in a paper Sutherland co-authored titled, "High-fidelity laser-free universal control of trapped-ion qubits." It was published in the scientific journal, *Nature,* on September 8.

Quantum computers have the potential to solve certain complex problems exponentially faster than classical super-computers.

One of the most promising uses for quantum computers is to simulate quantum mechanical processes themselves, such as chemical reactions, which could exponentially reduce the experimental trial and error required to solve difficult problems. These computers are being explored in many industries including science, engineering, finance and logis-tics.

"Broadly speaking, the goal of my research is to increase human control over quantum mechanics," Sutherland said. "Giving people power over a different part of nature hands them a new toolkit. What they will eventually build with it is uncertain."

That uncertainty, says Sutherland, is what excites him most.

Sutherland's research background includes quantum optics, which studies how quantum mechanical systems emit light. He earned his Ph.D. at Purdue University and went on to Lawrence Livermore National Laboratory for his postdoc, where he began working on experimental applications for quantum computers.

He became a tenure-track assistant professor at UTSA last August as part of the university's Quantum Computation and Quantum Information Cluster Hiring Initiative.

47. Berkeley Lab, 2 Universities to Collaborate on DOE-Backed Quantum Network Testbed Project

by Carol Collins
https://www.executivegov.com/2021/09/berkeley-lab-receives-12-5m-doe-funding-for-quantum-network-testbed-development/

The Department of Energy's (DOE) Lawrence Berkeley National Laboratory will collaborate with two research universities in California to develop a testing platform for the quantum internet concept under a five-year, $12.5 million project to be funded by DOE.

Berkeley Lab said its partnership with the University of California and the California Institute of Technology aims to produce a software-based distributed quantum computing network that will link the DOE facility and UC Berkeley.

The project, called Quantum Application Network Testbed for Novel Entanglement Technology, supports the federal government's National Quantum Initiative and is part of a $61 million DOE investment.

Other department funding awards include $12.5 million for a similar testbed development effort at Oak Ridge National Laboratory, $30 million for the establishment of five Nanoscale Science Research Centers and $5 million for the creation of continental-scale quantum internet building blocks.

Quantum networks use light's quantum properties for encoding more information compared to traditional computing technology, according to Berkeley Lab.

48. Fast quantum random number generator fits on a fingertip

by Pradeep Niroula
https://physicsworld.com/a/fast-quantum-random-number-generator-fits-on-a-fingertip/

Smartphones could soon come equipped with a quantum-powered source of random numbers after researchers in China developed a quantum random number generator (QRNG) chip small enough to sit comfortably on a fingertip. What's more, the new integrated photonic chip generates random numbers at rate of 18.8 gigabits per second – a record-high rate that should allow the generator to interface with the ever-increasing speed of Internet communications.

Random numbers are useful in cryptography and computer simulations, among other applications. For example, cryptography needs a source of true random numbers that a sophisticated adversary or eavesdropper cannot predict or manipulate. Similarly, true randomness ensures that computer simulation techniques, like the ones used for predicting weather or modelling protein molecules, produce accurate results.

For most purposes, wherever a high degree of randomness is not necessary, pseudo-random numbers suffice. These numbers appear random, but they are actually part of a sequence generated by a formula using a so-called seed number. This means that if hackers learn the seed number, they can predict the entire sequence of numbers, thus eliminating any randomness. A security protocol based on pseudo-random numbers is therefore weak since hackers might be able to guess the keys used for encryption.

On the other hand, true random numbers – ones that cannot be guessed or anticipated – are very hard to generate because they need a truly unpredictable origin. In their quest for true randomness, researchers have even turned to measuring cosmic radiation and observing patterns in volcanic lamps.

Turning quantum noise into usable randomness

Thankfully, there is also a more accessible source of true randomness: quantum superpositions. In quantum mechanics, a wavefunction can be in a superposition of many states and performing a measurement randomly collapses the wavefunction into one of those states. An electron, for example, can be in an equal superposition of "spin up" and "spin down" states, and measuring the electron gives one of the two spin states with 50% probability. It is almost like a coin-toss, except that a coin-toss is not really random since you can predict whether the coin lands heads or tails if you accurately account all forces on the coin (flick of the finger, wind movements, and so on). On the other hand, the measurement outcome of an electron in a superposition is simply unpredictable.

The QRNG developed by researchers at the University of Science and Technology in Hefei and Zhejiang University in Hangzhou uses a setup in which a reference laser beam is split into two and the intensity of the outgoing beams is measured using ultra-fast indium-gallium-arsenide photon detectors. The difference in the two intensities is affected by fluctuations in the so-called vacuum state, which is a quantum state that contains zero photons but still has some residual energy. When you try to measure the properties of this vacuum state, such as the magnitude of its electric field, Heisenberg's uncertainty principle guarantees that the results will, in theory, be random numbers picked from a normal distribution.

In practice, however, classical noise creeps in, giving the measurements unwanted bias and correlations that could help a hacker guess the generated numbers. To avoid this, the researchers used classical algorithms to remove unwanted correlations during post-processing, leaving only the true random numbers behind. These numbers were then transmitted to a personal computer where they passed a suite of tests showing that they are indeed random.

Random things in small packages

The security of small electronic gadgets has become more critical than ever due to the rise of the "Internet of Things" in which devices such as home appliances are connected to the Internet. QRNGs can protect such devices by supplementing conventional cryptography with truly random numbers. But to be useful, generators need to be fast enough to communicate over Wi-Fi or broadband internet. For this, a fast source of randomness is not enough on its own: the supporting photonic and electronic components used in post-processing and communication need to be just as quick. In addition, it should also be possible to embed the generator into small devices.

According to Jun Zhang, a physicist at Hefei and a co-author of the research published in *Applied Physics Letters*, the fabrication process developed by the Hefei-Hangzhou team solves this miniaturization challenge. Not only did the researchers achieve a record-high speed with their generator, they also managed to squeeze most of the critical components into an area of 15 mm^2, which is roughly one tenth the size of a micro-SIM card. While the current prototype chip still needs an external laser source and amplifiers, making the total package significantly larger, Zhang says the team intends to develop a low-cost version, albeit with a slower generation rate, for commercial use. If successful, such a chip would make true random numbers affordable enough for everyday laptops and smartphones.

49. Discovery Paves Way for Improved Quantum Computing Devices

by UNIVERSITY of QUEENSLAND
https://scitechdaily.com/discovery-paves-way-for-improved-quantum-computing-devices/

Physicists and engineers have found a way to identify and address imperfections in materials for one of the most promising technologies in commercial quantum computing.

The University of Queensland team was able to develop treatments and optimize fabrication protocols in common techniques for building superconducting circuits on silicon chips.

Dr. Peter Jacobson, who co-led the research, said the team had identified that imperfections introduced during fabrication reduced the effectiveness of the circuits.

"Superconducting quantum circuits are attracting interest from industry giants such as Google and IBM, but widespread application is hindered by 'decoherence', a phenomenon which causes information to be lost," he said.

"Decoherence is primarily due to interactions between the superconducting circuit and the silicon chip – a physics problem – and to material imperfections introduced during fabrication – an engineering problem.

"So we needed input from physicists and engineers to find a solution."

The team used a method called terahertz scanning near-field optical microscopy (THz SNOM) – an atomic force microscope combined with a THz light source and detector.

This provided a combination of high spatial resolution – seeing down to the size of viruses – and local spectroscopic measurements.

Professor Aleksandar Rakić said the technique enabled probing at the nanoscale rather than the macroscale by focusing light onto a metallic tip.

"This provides new access for us to understand where imperfections are located so we can reduce decoherence and help reduce losses in superconducting quantum devices," Professor Rakić said.

"We found that commonly used fabrication recipes unintentionally introduce imperfections into the silicon chips, which contribute to decoherence.

"And we also showed that surface treatments reduce these imperfections, which in turn reduces losses in the superconducting quantum circuits."

Associate Professor Arkady Fedorov said this allowed the team to determine where in the process defects were introduced and optimize fabrication protocols to address them.

"Our method allows the same device to be probed multiple times, in contrast to other methods that often require the devices to be cut up before being probed," Dr. Fedorov said.

"The team's results provide a path towards improving superconducting devices for use in quantum computing applications."

In the future, THz SNOM could be used to define new ways to improve the operation of quantum devices and their integration into a viable quantum computer.

50. Triple Qubit Entanglement Achieved in Research Breakthrough

by Francisco Pires
https://www.tomshardware.com/news/quantum-computing-triple-qubit-entanglement-achieved

Researchers with the Riken Center for Emergent Matter Science in Japan have demonstrated a triple-qubit, silicon-based quantum computing mechanism - opening up the road for increased scalability beyond a mere increment in total qubits on a given system. Previously, qubits had only been shown working in entangled pairs -- and this research demonstrates that entanglement (and thus computation) can actually be divided between three qubits.

Quantum computing rests atop qubits - the quantum equivalent of the modern transistor. But while typical transistors can only represent one value at any point in time (with that value being either zero or one), qubits benefit from the superposition mechanic of quantum physics, meaning that they can represent both states at the same time.

Until now, quantum computing systems worked by entangling two distinct qubits, which allowed them work in tandem in solving any complex workload (entanglement meaning that the qubits perfectly mirror each other, and any changes to one qubit's state are instantly replicated in the other). If you think of each qubit as a single core, the research now increases the maximum amount of qubits ("cores") that can work in synchrony to be three, from its previous two-qubit maximum. Theoretically, you can now build multiple triple-core quantum computing subdivisions, instead of dual-core ones.

This research thus has several implications in quantum scaling, as well as in the complexity of quantum algorithms. Seigo Tarucha, one of the researchers involved, explains that "(...) two-qubit operation is good enough to perform fundamental logical calculations, but a three-qubit system is the minimum unit for scaling up and implementing error correction."

The researchers used one of the approaches currently being explored as enablers for quantum computing: a trio of silicon quantum dots, which are built out of a silicon/silicon–germanium heterostructure and are controlled through aluminum gates. Each silicon quantum dot features a single electron (negatively charged particles) which changes its spin states in response to a strong, on-chip magnet. The magnet generates a magnetic-field gradient which in turn separates the resonance frequencies of the three qubits, allowing them to be individually addressed.

This has important implications for error correcting of results. Turing machines like our personal computers already have deep error correction protocols inside them, which ensure the validity of calculations. This error correction requirement is still in its infancy in the quantum field, which is why this demonstration is so important. As per the researchers' approach, the third qubit can now be used as an aide in calculations, helping achieve a remarkably high (for quantum computing) state fidelity of 88%.

As with everything relating quantum computing, which is still in its nascent phase, scalability is the keyword here, and the researchers will continue to explore what they theorize can already be achieved with their technique.

“We plan to demonstrate primitive error correction using the three-qubit device and to fabricate devices with ten or more qubits," said Tarucha. "We then plan to develop 50 to 100 qubits and implement more sophisticated error-correction protocols, paving the way to a large-scale quantum computer within a decade.” The world awaits.

51. Microsoft President Brad Smith warns that U.S. is repeating a key Sept. 11 mistake in digital era

by TODD BISHOP
https://www.geekwire.com/2021/microsoft-president-brad-smith-warns-u-s-repeating-key-sept-11-mistake-digital-era/#news-stream

Microsoft President Brad Smith says the U.S. government appears to be repeating, in the digital realm, one of the key missteps that preceded the Sept. 11 attacks.

Tightly controlled silos of information about cyberattacks persist among U.S. government agencies, Smith writes in a new update to his book, *Tools and Weapons: The Promise and the Peril of the Digital Age,* originally published two years ago.

"It's impossible to avoid the grave conclusion that the sharing of cybersecurity threat intelligence today is even more challenged than it was for terrorist threats before 9/11," writes Smith, with co-author Carol Ann Browne, in one of three new chapters in the paperback edition of the book, released Tuesday.

One anecdote illustrates the challenge from Microsoft's perspective:

"Repeatedly in late 2020 we found people in federal agencies asking us about information in other parts of the government, because it was easier to get it from us than directly from other federal employees. A culture of holding information tightly is so ingrained in the government that even its contracts with us forbid us from letting one part of the government know that another part has been attacked."

That gets to the larger takeaway from the updated book: we've all still got a lot to learn in the digital age — Microsoft and other big tech companies included — and the lessons are hitting us faster than we ever imagined.

SolarWinds attack: Nowhere is that more evident than in the fallout from the SolarWinds attack, which is the subject of a new opening chapter of the book.

Smith details Microsoft's response to the attack, believed to be launched by a Russian hacking group, saying the company assigned more than 500 employees "to work full-time on every aspect of the attack" in the early days. Microsoft CEO Satya Nadella convened a daily meeting with the company's top security experts.

Microsoft's own investigation found evidence of malicious code on its own network, but Smith reiterates the company's past statements that the attackers were not able to change source code, access customer data or production services, or use Microsoft's systems to attack others.

Smith explains that the attackers "shrewdly used American data centers to help cloak the attacks," hosting the command-and-control servers at GoDaddy and Amazon Web Services in an apparent attempt to avoid raising the suspicions of the National Security Agency, which has the authority to scan foreign but not domestic online activity.

Microsoft took control of one of the servers from GoDaddy, and security teams were able to activate a kill switch in the malware, limiting the attacks, he writes.

He also underscores the importance of more information sharing by companies about security breaches, which was a focus of a recent White House summit.

Software and the cloud: In other situations, Microsoft's own software has been part of the problem, including an attack by a Chinese-sponsored group exploiting vulnerabilities in the company's Exchange Server software.

Big picture, one of Smith's proposed solutions is to move more software to the cloud, taking the responsibility for implementing patches away from individual people and companies — which he concedes isn't a surprising position from an executive at a major cloud technology company.

"As I acknowledged to the Senate Intelligence Committee, there's always the danger that a hammer will see everything as a nail," he writes. "But from our perspective, these episodes clearly told us that it's far better for most customers to modernize their technology infrastructure by migrating to the cloud and relying on the cybersecurity expertise of companies that make this part of their core competency."

Pence's miscalculation: Under normal circumstances, a tech company would welcome a U.S. vice president encouraging organizations to use its software for some high-profile purpose.

But Microsoft executives "virtually fell off our chairs" when they saw a letter from then-Vice President Mike Pence directing individual hospitals across the country to send daily reports to the White House using an Excel spreadsheet, Smith writes.

"It not only failed to use the right data-analytics tools," Smith writes, "but sought to collect at a national level data that was far easier to ask the counties and states to collect, for eventual national aggregation."

Technology in the pandemic: One new chapter focuses on the impact of COVID-19 on work and life around the globe. Smith draws insights from the aftermath of World War II to caution against believing "overly exuberant" predictions of a wholesale shift to virtual work, for example.

The reality, he says, is somewhere in between.

"When we step back and consider technology trends more broadly, it is apparent that people will have more choices about how to live their lives," he writes. "This means that people will have the flexibility to choose among the best of both online and in-person interaction, blending different experiences to meet different needs."

52. Quantum Leadership in Action: An Interview with Dr. Prineha Narang

by Kenna Castleberry
https://thequantumdaily.com/2021/09/07/quantum-leadership-in-action-an-interview-with-dr-prineha-narang/

Within the deep tech industry, quantum technology is gaining significant interest from both investors and the general public. Current quantum technology companies cover a wide variety of markets, from quantum computing to quantum encryption to quantum networking. All of these businesses are working hard to make future technology more accessible.

One of these quantum networking companies is Aliro Quantum. Founded in 2019, Aliro's technology originated in the laboratory of Harvard professor, Dr. Prineha Narang. Narang is also currently the CTO of Aliro, responsible for a wide range of functions from R&D to marketing strategies. "My role within Aliro is really kind of all-encompassing," Narang explains. "This is what it means to be the CTO of a startup, as I help with tasks ranging from architecture to software to the day-to-day technology aspects, talking to investors, talking with potential partners, various big network service providers, or big utility companies. It's perhaps a little bit different from what one imagines for the CTO of a big company, but within a startup, you really have to do everything." Thanks to Narang and the team's hard work, Aliro is a big player in the quantum technology market, providing foundational technologies to build complex quantum

network systems in the commercial sector. Since 2019, Alito has partnered with IBM Q Network, Honeywell Quantum Solutions, ESNet, and Hyperion research, as well as many more businesses.

In founding Aliro, Narang notes a natural connection between her Harvard lab and her new company. Narang clarified the technology of Aliro as: "building the entire quantum network stack, thinking about how we can realize various core network pieces. People talk about all the layers that you have in a network: layer one, layer two, and how you actually eventually connect up to an application. And developing that for quantum networks has been really exciting." Not only does she enjoy working on the innovative technology, but Narang also finds she enjoys the quick pace of a startup company, even if it does make her workday busier. "From a day-to-day standpoint, I need to manage my time very, very well. I frequently noticed that any scheduled meeting will likely take up all the schedule time. So, I try to remain cognizant in terms of a deadline. My research group is pretty big. we're on the order of 16 to 17 people now, and Aliro, of course, is pretty sizable!" By developing a routine that works for her, Narang is able to be a successful CTO and Harvard professor simultaneously.

From her role as a CTO, Narang is able to translate many of her industry "real-world" skills to her mentoring as a professor. "I think that I've been able to bring a different perspective to my mentoring, teaching, and the classroom because of this connection with both Aliro and other parts of the quantum industry. In academia, industry, and national labs, I think quantum is one of those fields where you could do really spectacular science and technology, regardless of which of those paths you pick. I've been able to share this with my Ph.D. students and mentor them in a way that a traditional academic might not have been able to previously." Using her knowledge of the industry, Narang believes she's able to give her students timelier guidance when determining their future careers.

While Aliro did originate out of Narang's laboratory at Harvard, her research is much broader than the work being done at Aliro. Many things are synergistic. For example, Narang and her team at Harvard are looking at future quantum memories, specifically at quantum defects in solids to realize scalable quantum networks. She believes this research can help develop long-range quantum networks. Narang is also looking at quantum correlations in the matter. "So, essentially, we can use quantum probes, like quantum sensing, as a probe of correlated transport in quantum matter, and we have a few different papers on unconventional transport in quantum matter that are out and some that are coming out very soon." Should Narang's team find methods to develop quantum memories for larger quantum networks, these methods could be applied to Aliro, and the company could become an even bigger name in quantum technology.

Narang has a unique appreciation for research at the intersection of theory and experiment, "co-design" of quantum technologies. Narang originally worried about being a theorist but found that "theorists actually are the most interactive people. There's so much that happens over good coffee and a blackboard, where somebody is writing out an equation and discussing it." From her interest, in theory, Narang then moved into quantum information science, "I started playing around with GPU accelerated computational methods in grad school, and eventually realized that programming quantum devices and using them to compute interesting correlations- understanding physics with this new tool is actually a natural progression." From there, her work became successful to the point when she founded Aliro.

Moving forward, Narang hopes to inspire others to consider quantum and quantum technology as viable career opportunities. Being one of a few women CTOs in the industry (only two on this list), Narang hopes to inspire more inclusivity. "I want to encourage people who might not see somebody who looks like them in the field right now, to take the leap say that this is a field that is welcoming. There is a lot of support once people are in the field. This field *IS* for women and for underrepresented minorities, though, of course, from the outside, it may seem a little bit daunting." Narang recounts her own experiences, saying she didn't see many people with her background early on after joining the quantum field. Thanks to mentors who showed her support, Narang found a welcoming community. "That would be my message to others who are considering joining this field: you absolutely belong. And I hope you will consider joining this field."

53. Quantum Computing Breakthrough: Entanglement of Three Spin Qubits Achieved in Silicon

by RIKEN
https://scitechdaily.com/quantum-computing-breakthrough-entanglement-of-three-spin-qubits-achieved-in-silicon/?utm_medium=email&_hsmi=165004420&_hsenc=p2ANqtz-_sVUwX2BNT-nEbbKhfjso4tWCqvlBnMg2q3vHPD3Bq697bXgkD214xFYdRiGtRr-RYg0XE7DuFHcZTr7oMu-xX9LGWGwTA&utm_content=165004420&utm_source=hs_email

A three-qubit entangled state has been realized in a fully controllable array of spin qubits in silicon.

An all-RIKEN team has increased the number of silicon-based spin qubits that can be entangled from two to three, highlighting the potential of spin qubits for realizing multi-qubit quantum algorithms.

Quantum computers have the potential to leave conventional computers in the dust when performing certain types of calculations. They are based on quantum bits, or qubits, the quantum equivalent of the bits that conventional computers use.

Although less mature than some other qubit technologies, tiny blobs of silicon known as silicon quantum dots have several properties that make them highly attractive for realizing qubits. These include long coherence times, high-fidelity electrical control, high-temperature operation, and great potential for scalability. However, to usefully connect several silicon-based spin qubits, it is crucial to be able to entangle more than two qubits, an achievement that had evaded physicists until now.

Seigo Tarucha and five colleagues, all at the RIKEN Center for Emergent Matter Science, have now initialized and measured a three-qubit array in silicon with high fidelity (the probability that a qubit is in the expected state). They also combined the three entangled qubits in a single device.

This demonstration is a first step toward extending the capabilities of quantum systems based on spin qubits. “Two-qubit operation is good enough to perform fundamental logical calculations,” explains Tarucha. “But a three-qubit system is the minimum unit for scaling up and implementing error correction.”

The team’s device consisted of a triple quantum dot on a silicon/silicon–germanium heterostructure and is controlled through aluminum gates. Each quantum dot can host one electron, whose spin-up and spin-down states encode a qubit. An on-chip magnet generates a magnetic-field gradient that separates the resonance frequencies of the three qubits, so that they can be individually addressed.

The researchers first entangled two of the qubits by implementing a two-qubit gate—a small quantum circuit that constitutes the building block of quantum-computing devices. They then realized three-qubit entanglement by combining the third qubit and the gate. The resulting three-qubit state had a remarkably high state fidelity of 88%, and was in an entangled state that could be used for error correction.

This demonstration is just the beginning of an ambitious course of research leading to a large-scale quantum computer. "We plan to demonstrate primitive error correction using the three-qubit device and to fabricate devices with ten or more qubits," says Tarucha. "We then plan to develop 50 to 100 qubits and implement more sophisticated error-correction protocols, paving the way to a large-scale quantum computer within a decade."

54. Chinese Scientists Say Quantum Radar Could End Stealth Advantage

by Matt Swayne
https://thequantumdaily.com/2021/09/04/chinese-scientists-say-quantum-radar-could-end-stealth-advantage/

A new quantum radar technology developed by a team of Chinese researchers would be able to detect stealth planes, the South China Morning Post is reporting.

The news service reports that the radar technology generates a mini electromagnetic storm to detect objects. Professor Zhang Chao and his team at Tsinghua University's aerospace engineering school, reported their findings in a paper in Journal of Radars.

A quantum radar is different from traditional radars in several ways, according to the paper. While traditional radars have on a fixed or rotating dish, the quantum design features a gun-shaped instrument that accelerates electrons. The electrons pass through a winding tube of a strong magnetic fields, producing what is described as a tornado-shaped microwave vortex.

The researchers said they tested a smaller scaled version of the radar.

Taking the step from theoretical stealth-detecting quantum radar and small-scale prototypes to an actual device will not be an easy task, the researchers suggest. According to the newspaper, they are looking for industrial partners to build a full-sized version.

This isn't the first time Chinese scientists have said they have developed a quantum radar, or created a device that can undermine stealth technology. In 2016, scientists reported they could detect stealth aircraft.

Other scientists aren't sure that the approach will ever pan out.

"There's just a lot of problems that make it hard for me to believe that this system is going to be of any use," said Jeffrey Shapiro, an MIT professor and one of the first physicists who came up with the idea of quantum radar, in an interview with Science magazine last year.

55. TensorFlow Quantum v2, Quantify-Core 0.5, and Cirq 1.0 Roadmap

https://quantumcomputingreport.com/new-software-releases-tensorflow-quantum-v2-quantify-core-0-5-and-cirq-1-0-roadmap/

TensorFlow Quantum is an open source library for quantum machine learning originally released by Google in 2020. It is a follow-on to the original TensorFlow program written for classical computers that was released in 2017. It offers high-level abstractions for the design and training of both discriminative and generative quantum models under TensorFlow and supports high-performance quantum circuit simulators. It allow one to rapidly prototype quantum ML models. Version 2 contains a number of new features including bigger gate fusions, GPU CUDA support, adjoint differentiation, noisy simulations and more. An updated white paper that describes TensorFlow Quantum along with the new features is available there, a web page that contains several videos that help explain it is available here, and the GitHub repository for Tensor Flow Quantum is available here.

Quantify-Core is open source software developed by Qblox and Orange Quantum Systems to provide a tool for data acquisition for quantum computing and solid-state physics experiments. New version 0.5 has been released with a number of new features. For details you can view a short release announcement here, the changelog for the software here, and the user guide here.

Cirq is a Python software library for writing, manipulating, and optimizing quantum circuits, and then running them on quantum computers and quantum simulators. Cirq provides useful abstractions for dealing with today's noisy intermediate-scale quantum computers, where details of the hardware are vital to achieving state-of-the-art results. Although it was originally written to support Google's own superconducting based quantum computer, various backends have been written to support other machines such as the machines from Rigetti, IonQ, and AQT. To provide for better visibility for Cirq users, Google has published a roadmap for Cirq 1.0 that describes specific developments with classifcations that separate them into Released, Finished, We're Working on It, and Planned. You can view this roadmap here, a web page that provides various tutorials and overviews here, and the GitHub page here.

56. AMD files teleportation patent to supercharge quantum computing

by Katie Wickens

https://www.pcgamer.com/uk/amd-teleportation-quantum-computing-multi-simd-patent/

AMD has proposed a patent for 'teleportation,' meaning things could be about to get much more efficient around here. With the incredible technological feats humanity achieves on a daily basis, and Nvidia's Jensen going off on one last year about GeForce holodecks and time machines, it's easy for us to slip into a headspace that lets us believe genuine human teleportation is just around the corner.

"Finally," you sigh, mouthing the headline to yourself. "Goodbye work commute, hello popping to Japan for an authentic Ramen on my lunch break."

I'm sorry to say the reality is much less... palpable.

Our colleagues over at Tom's Hardware spotted the new patent lain down by AMD engineers, named 'Look-ahead teleportation for reliable computation in multi-SIMD quantum processor.' As the title suggests, it looks like the company has been researching systems involving quantum teleportation processes. The aim is to improve the current reliability of quantum computing, and even reduce the number of qubits necessary to make accurate calculations.

57. Researchers find a way to check that quantum computers return accurate answers

by University of Vienna
https://www.sciencedaily.com/releases/2021/09/210903132631.htm

Quantum computers are advancing at a rapid pace and are already starting to push the limits of the world's largest supercomputers. Yet, these devices are extremely sensitive to external influences and thus prone to errors which can change the result of the computation. This is particularly challenging for quantum computations that are beyond the reach of our trusted classical computers, where we can no longer independently verify the results through simulation. "In order to take full advantage of future quantum computers for critical calculations we need a way to ensure the output is correct, even if we cannot perform the calculation in question by other means," says Chiara Greganti from the University of Vienna.

Let the quantum computers check each other

To address this challenge, the team developed and implemented a new cross-check procedure that allows the results of a calculation performed on one device to be verified through a related but fundamentally different calculation on another device. "We ask different quantum computers to perform different random-looking computations," explains Martin Ringbauer from the University of Innsbruck. "What the quantum computers don't know is that there is a hidden connection between the computations they are doing." Using an alternative model of quantum computing that is built on graph structures, the team is able to generate many different computations from a common source. "While the results may appear random and the computations are different, there are certain outputs that must agree if the devices are working correctly."

A simple and efficient technique

The team implemented their method on 5 current quantum computers using **4 distinct hardware technologies**: superconducting circuits, trapped ions, photonics, and nuclear magnetic resonance. This goes to show that the method works on current hardware without any special requirements. The team also demonstrated that the technique could be used to check a single device against itself. Since the two computations are so different, the two results will only agree if they are also correct. Another key advantage of the new approach is that the researchers do not have to look at the

full result of the computation, which can be very time consuming. "It is enough to check how often the different devices agree for the cases where they should, which can be done even for very large quantum computers," says Tommaso Demarie from Entropica Labs in Singapore. With more and more quantum computers becoming available, this technique may be key to making sure they are doing what is advertised.

Academia and industry joining forces to make quantum computers trustworthy

The research aiming to make quantum computers trustworthy is a joint effort of university researchers and quantum computing industry experts from multiple companies. "This close collaboration of academia and industry is what makes this paper unique from a sociological perspective," shares Joe Fitzsimons from Horizon Quantum Computing in Singapore. "While there's a progressive shift with some researchers moving to companies, they keep contributing to the common effort making quantum computing reliable and useful."

58. NSA doesn't think quantum computers can break public key encryption

by Mayank Sharma
https://www.msn.com/en-us/news/technology/nsa-doesnt-think-quantum-computers-can-break-public-key-encryption/ar-AAO4Egk

The US National Security Agency (NSA) isn't really sure when or even if quantum computers will be able to crack public key cryptography.

Post-Quantum Cryptography is an emerging field of research, with researchers devising mechanisms to shore up current encryption algorithms against the seemingly unlimited computing performance promised by quantum computers.

The NSA however has expressed its reservations about the potential of quantum computing in a FAQ titled Quantum Computing and Post-Quantum Cryptography.

"NSA does not know when or even if a quantum computer of sufficient size and power to exploit public key cryptography (a CRQC) will exist," said the security agency in response to whether it is worried about the potential of adversarial use of quantum computing.

Encryption isn't the weakest link

Public-key encryption drives most of the standards and protocols on the internet and the cloud, which help ensure the integrity of the data even when it's been hijacked by snoopers.

In the FAQ, the NSA describes a Cryptographically Relevant Quantum Computer (CRQC) as a quantum computer that's capable of actually attacking real world cryptographic systems, something that's currently infeasible.

While it agrees that such a computer would be "devastating" to the digital security infrastructure, it seems to suggest that it doesn't believe such a CRQC would ever materialize.

However, the growing research in quantum computing has moved the agency to also support the development of post-quantum cryptographic standards, along with plans for eventual transition to such standards.

However, speaking to industry experts, *The Register* concludes that research on cryptography standards aren't much of a concern to cybersecurity specialists.

"In a world where users will divulge their passwords in return for chocolate or in response to an enticing phishing email, the risk of quantum computers might not be our biggest threat," Martin Lee, a technical lead at Cisco's Talos security division told *The Register*.

59. U.S. National Security Agency Issues Update on Quantum-Resistant Encryption

by Francisco Pires
https://www.tomshardware.com/news/us-national-security-agency-issues-update-on-crypto-resistant-encryption?utm_medium=email&_hsmi=165004420&_hsenc=p2ANqtz-8q4ksdoqFKBivtao-E8CHiUE0O0QXLEr469yXNUmeK6XY-pvqG2CjhvsXCwihWhUOw4QAzlOGEve0x0CxrXjCiJvkbETw&utm_content=165004420&utm_source=hs_email

The U.S. National Security Agency (NSA) has issued a FAQ (PDF) titled "Quantum Computing and Post-Quantum Cryptography FAQs" where the agency explores the potential implications for national security following the likely arrival of a "brave new world" beyond the classical computing sphere. As the race for quantum computing accelerates, with a myriad of players attempting to achieve quantum supremacy through various, exotic scientific investigation routes, the NSA document explores the potential security concerns arising from the prospective creation of a "**Cryptographically Relevant Quantum Computer**" (CRQC).

A CRQC is the advent of a quantum-based supercomputer that is powerful enough to break current, classical-computing-designed encryption schemes. While these schemes (think AES-256, more common on the consumer side, or RSA 3072-bit or larger for asymmetrical encryption algorithms) are virtually impossible to crack with current or even future supercomputers, a quantum computer doesn't play by the same rules due to the nature of the beast and the superposition states available to its computing unit, the qubit.

With the race for quantum computing featuring major private and state players, it's not just the expected $26 billion value of the quantum computing sphere by 2030 that worries security experts - but the possibility of quantum systems falling into the hands of rogue entities. We need only look to the history of hacks in the blockchain sphere to see that

where there is an economic incentive, there are hacks - and data is expected to become the number one economic source in a (perhaps not so) distant future.

Naturally, an entity such as the NSA, which ensures the safety of the U.S.'s technological infrastructure, has to not only deal with present threats, but also future ones - as one might imagine, it takes an inordinate amount of time for entities as grand as an entire country's critical government systems to be updated.

According to the NSA, "*New cryptography can take 20 years or more to be fully deployed to all National Security Systems (NSS)". And as the agency writes in its document*, "(...) *a CRQC would be capable of undermining the widely deployed public key algorithms used for asymmetric key exchanges and digital signatures. National Security Systems (NSS) — systems that carry classified or otherwise sensitive military or intelligence information — use public key cryptography as a critical component to protect the confidentiality, integrity, and authenticity of national security information. Without effective mitigation, the impact of adversarial use of a quantum computer could be devastating to NSS and our nation, especially in cases where such information needs to be protected for many decades.*"

The agency's interest in quantum computing is such, even, that as a part of the document trove leaked by Edward Snowden, it was revealed that the agency invested $79.7 million in a research program titled “Penetrating Hard Targets” - which aimed to explore whether a quantum computer for actually breaking traditional encryption protocols was feasible to pursue at the time.

This is especially important considering that an algorithm that can be employed by a quantum computer to break traditional encryption schemes already exists in the form of Schor's algorithm, first demonstrated in 1994 - before humanity's control over the qubit was all but a distant dream. The only thing standing in the way of the Schor algorithm's implementation at a quantum level is that it requires a much larger amount of qubits than is currently feasible - orders of magnitude higher than today's most advanced quantum computing designs, that max out at around "only" one hundred qubits.

It is only a matter of time, however, before such systems exist. The answer lies in the creation and deployment of so-called post-quantum cryptography - encryption schemes designed to give pause to or even completely thwart future CRQCs. These already exist. However, their deployment at a time where the cryptographic security threat of quantum computing still lays beyond the horizon, implementing post-quantum cryptography would present issues in terms of infrastructure interoperability - different systems from different agencies and branches sharing confidential information between themselves and understanding what they're transmitting between each other.

In its documentation, NSA puts the choice on exactly what post-quantum cryptography will be implemented by the U.S. national infrastructure on the feet of the National Institute of Standards and Technologies (NIST), which is "*in the process of standardizing quantum-resistant public key in their Post-Quantum Standardization Effort, which started in 2016. This multi-year effort is analyzing a large variety of confidentiality and authentication algorithms for inclusion in future standards,*" the NSA writes.

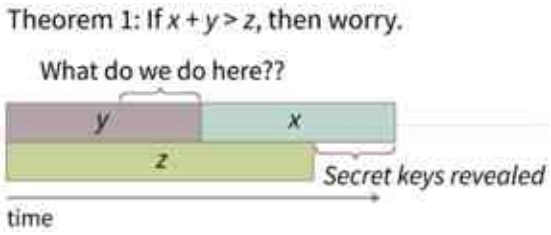
But contrary to what some would have you think, the NSA knows that it's a matter of time before quantum computing turns the security world on its proverbial head. There's no stopping the march of progress; as the agency writes, "The intention is to (...) remove quantum-vulnerable algorithms and replace them with a subset of the quantum-resistant algorithms selected by NIST at the end of the third round of the NIST post-quantum effort."

60. The Battle For Post-Quantum Security Will Be Won by Agility

by Thomas Poeppelmann and Martin Schlaeffer
https://semiengineering.com/the-battle-for-post-quantum-security-will-be-won-by-agility/

Due to their special features, quantum computers have the disruptive potential to replace existing conventional computers in many applications. They could, for example, calculate simulations of complex molecules for the chemical and pharmaceutical industry, perform complicated optimizations for the automotive and aviation industry, or create new findings from the analysis of complex financial data. At the same time, quantum computers also raise a lot of security concerns, and while today they don't have real world applications, their capabilities are expected to grow significantly over the next 10 years. According to Michele Mosca, there is only a 14% chance that RSA2048 will be broken by 2026, but that grows to 50% by 2031. The security community has taken notice and is already preparing for quantum attacks.

The challenge is we don't yet know which will become the standard, but thanks to Mosca's Theorem, we know we need to start preparing now. According to Mosca, when $X+Y>Z$ (where X is the shelf life of your data; Y is the time it will take to transfer your data; Z is the number of years until stable quantum computers become available), it is time to worry. In other words, that 10-year runway we think we have is actually significantly less.



An additional challenge is that we don't yet understand how powerful subsequent generations of quantum computers will be. This makes it impossible to be completely certain if a specific approach will work or how long it will last. The key will be cryptographic agility.

As laid out in Mosca's Theorem, there are many data sets that exist today that, due to company data retention policies or regulatory requirements, will need to be kept confidential and protected against manipulation past the time we expect quantum attacks to be a threat. For that data, it's not possible to wait for quantum resistant cryptography standards to be developed.

The National Institute for Standards and Technology (NIST) started a Post Quantum Cryptography (PQC) standardization process in 2016 to prepare quantum resistant crypto algorithms. Since most symmetric primitives are relatively easy to modify in a way that makes them quantum resistant, efforts have focused on public-key cryptography, namely digital signatures and key encapsulation mechanisms. Now more than six years into the process, there is discussion whether the process related to digital signatures should be opened up again or needs more time.

For some applications, hash-based signatures, which are ready and already standardized can be a good solution. They are regarded as very secure and quantum resistant, due to their one-way function, and may be used to achieve long term integrity and authenticity of data. Due to this attribute, the secret key is very well protected, as obtaining the secret keys from a public key would require breaking of a modern cryptographic hash function – a well understood and very hard problem. Hash-based signature algorithms consist of large hash trees and hash chains, making them ideal for a number of applications, such as firmware updates. It is computationally expensive to build a hash tree, in which each key (known as a leaf) is assigned a secret key, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Additionally, because each leaf is a unique private key for each sign operation, it can only be used once. Thus, the larger the number of keys that are needed, the larger the tree. This has a direct and significant impact on how long it takes to generate the required number of keys, adds computational expense and can even impact network performance. That said, once built it provides an efficient algorithm for signing and leads to fast verification times.

For applications that aren't well-suited for hash-based algorithms, there is currently no standardized algorithm that could be used out of the box. Companies must continue to develop devices and need to include cryptography as part of the security mix. The question these companies face is what algorithm should they choose when it's unclear:

- What the PQC standard will be
- How that standard might need to change as classical and quantum attacks become more powerful

Any post-quantum cryptography (PQC) algorithm we create today will likely become obsolete eventually. We've seen it happen before. One example occurred in 2017 when Google, along with CWI, announced a public collision in the SHA-1 algorithm – a deathblow to the one-time most popular hash algorithm. While the breaking of an encryption is scary itself, researchers generally have a pretty good idea of when we're getting close to breaking it and developing a stronger alternative in time. What's more concerning is that cryptographic algorithms are deeply integrated into the system and it can be extremely hard to move on to a new scheme – a fact that may leave systems vulnerable.

That was the scenario that played out in 2004 when the MD5 algorithm was broken. It took four years until researchers demonstrated a practical attack, four more years until a large-scale attack was carried out in practice. Nevertheless, two years later some companies reportedly forced their clients to transition within a few months. In total, it took more than 10 years from the time MD5 was first widely known to be vulnerable to remove it from use because the transition was so painful it took a forcing function to make it happen.

That's where crypto agility is gaining interest. It is essentially the ability to remove old broken algorithms and plug in new stronger versions.

The effort to achieve post quantum security will rely on currently available quantum resistant solutions, such as hash-based signatures for firmware updates, as well as new technologies. As we look to the future of a quantum computing world and start preparing for it, it will be even more important to embrace crypto agility. There will be legacy systems running a certain set of non-quantum safe algorithms. At some point in the future, there will be new algorithms that have to be integrated. For a system to survive this migration, it needs to be designed in a way to be crypto agile, where the crypto functions are separate blocks and where they can be exchanged. Without crypto agility we would be faced with a reality where systems would essentially have to be disposable – where every time a crypto algorithm is broken, we throw them away or never update them. This isn't a realistic option for complex and expensive systems.

As with most things in life, what a post-quantum world will look like is filled with uncertainty. Uncertainty on what PQC standards will be made. Uncertainty on how powerful quantum computers will be. And uncertainty on what new discoveries will be unlocked. One thing that is certain – security must be kept up to date to meet continuingly advanced attacks and the only way to do that is by embracing crypto agility. This is leading forward-thinking semiconductor

and computing device manufactures – who take security seriously – to invest in critical technology now, which will enable their customers to address Mosca's theorem and the challenge of quantum technologies.

61. DANGERS of QUANTUM HACKING: A THREAT to ENCRYPTION

by Aratrika Dutta
https://www.analyticsinsight.net/dangers-of-quantum-hacking-a-threat-to-encryption/

Quantum computers have limitless potentials. There is no doubt that one day quantum computers will find a cure for cancer or help in eliminating world hunger. But along with this, they could also help hackers get access to our most private data by breaking encryption. While quantum computing is beneficial, quantum hacking is dangerous.

What is quantum hacking?

To be precise quantum hacking is the use of quantum computers to carry out malicious actions. Quantum hacking is performed by modern cryptographic strategies which often use private and public keys to encrypt and decrypt data through a mathematical equation. These mathematical equations can be easily broken by advanced quantum computers. It would surely take a while, but the process is still possible using the nonlinear protocol of quantum computing.

When quantum hacking becomes possible, a system that repairs the existing internet security practices needs to be developed. If not, it would be easy for hackers to break through data and cause costly issues.

Threat to Encryption

With digital transformation, everything is now digital, even data, and all our digital data like emails, chats, online purchases, etc are encrypted which makes it unreadable without a decryption key. This prevents our data in the cloud and our computers from being tampered with. AES (Advanced Encryption Standard) is the most commonly used method for encrypting all this data. With today's classical computers it is impossible to break AES encryption, but through quantum computers, it is possible to decrypt the encrypted data.

It is believed that quantum-optimized algorithms and artificial intelligence will increasingly be used together in breaking the mathematically based cryptographic algorithms. While performing a huge superposition of possible results to these algorithms requires a quantum device in the millions of qubits and the largest quantum computer today has just 72 qubits, similar results can be obtained with quantum-optimized algorithms performing within a computer emulator running on consumer gaming video cards.

With advanced quantum computing and with readily available hardware paired with new software processor-heavy brute force hacking techniques can be done much faster.

There is an increasing fear among cybersecurity specialists that quantum computing will result in the nightfall of the existing encryption standard which means one day all encrypted files could be decrypted one day. Already hackers have been using mobile devices that can collect credit card information with the credit card holder being unnoticed.

Therefore quantum computing devices will open the door for remarkably more cyberthreats. There are numerous benefits of quantum computing but if it falls into the hands of malicious actors then it would be dangerous.

Already hackers have stolen encrypted data, now it's time to wait for the day when they can use quantum computers to decode those files. Everything is vulnerable, from financial statements to healthcare records. It is required for governments and businesses as well as consumers to take action to protect their data.

Is Prevention Possible?

Experts say that quantum hacking is only preventable if quantum cryptography encryption keys are so entangled that even the most advanced quantum computers cannot break them. The only drawback to this is that continual encryption would lead to very lengthy keys that would ultimately slow down the process.

While engineers are focused on developing the most advanced quantum computer, cybersecurity specialists are emphasizing bringing out a new form of cryptography that would protect against quantum hacks. This is known as post-quantum cryptography or PQC. Experts are presently creating PQC solutions, but these will need to be regulated and widely adopted.

62. A Classiq Solution to a Current Quantum Challenge

by Matt Swain
https://thequantumdaily.com/2021/09/01/tqd-exclusive-a-classiq-solution-to-a-current-quantum-challenge/

Even if hardware advances can create quantum computers with hundreds, thousands, or even millions of qubits, the complexity of circuit design for those computers may mean that quantum advantage will remain a distant dream. Tel-Aviv-based Classiq is working to change that.

The Classiq approach, called "Quantum Algorithm Design," automatically synthesizes optimized quantum circuits from high-level functional models. The solution was born from the founders 'desire to solve problems that are limiting progress in quantum, explained Nir Minerbi, Classiq co-founder and CEO.

"When we explored the quantum industry to identify its main bottlenecks, it became clear that software is a big challenge," said Minerbi. "We trust the tech giants to deliver more powerful hardware, but currently, the quantum software stack is in its infancy. Developing quantum software is almost an impossible task"

Minerbi estimates that only a few thousand people in the world can design a 10-qubit quantum circuit. That number falls to a few hundred experts who can design a 50-qubit circuit.

"And it becomes increasingly unlikely that anyone can develop circuits beyond 50 qubits," said Minerbi. "But how about designing 100-, 500- or 10,000-qubit quantum circuits? That's a very complex challenge with existing tools. So, that became Classiq's vision: to solve this problem and to enable the software to scale alongside the hardware."

According to Minerbi, solving the design complexity problem does more than just make quantum computers more practical — it makes them more accessible. With Classiq, organizations can combine the power of elite quantum scientists with domain-specific experts as well as other individuals within their enterprises. These integrated teams can engineer solutions to the world's most pressing problems.

"We want to enable the quantum experts to do the high-level design, but, in parallel, enable domain experts who are not quantum specialists to participate in and contribute to the quantum algorithm design process," said Minerbi. "That's what some of our customers are doing today. We see more and more teams with between one and ten quantum information Ph.D.'s alongside people from other business units who are not quantum experts."

Not a New Problem

There's an analog to this approach in classical electronic circuit design, Minerbi explained.

"If you want to design a simple electronic chip with storage, a simple printed circuit with a few dozens of classical gates — like AND gates and NOT gates — that's a complex design problem, but you can still do it manually," said Minerbi. "However, you can't design circuits with millions or billions of transistors in the same way. Luckily, you don't need to because, in the classical electronic design process, there are high-level modeling languages like VHDL and Verilog that define what functionality you want to achieve out of the circuit without requiring you to define the implementation."

Then, there are software platforms like Cadence or Synopsis that read these high-level models and synthesize a circuit that meets your demands and constraints. These platforms allow the users to define what functionality they want to achieve without requiring them to define all the details about the implementation.

In Classiq's quantum version, the implementation of this gate-level circuit is automated by the company's software. The software acts like "VHDL for Quantum," injecting a high-level functional model and turning it into a gate-level quantum design. According to the company, this ultimately puts the power of quantum computers in the hands of more people, who can then use their creativity and knowledge to enable quantum solutions for a wide variety of industries and use cases.

To allow creating solutions using today's NISQ-era computers, Classiq also makes it easy to create hybrid solutions that combine quantum computing with classical processing.

Satisfying the designer's requirements and constraints

The Classiq platform gets inputs from a high-level functional model and the constraints the designer needs to meet. It uses a constraint satisfaction engine to fulfill the requirements while meeting the constraints.

Minerbi explained: "The constraint satisfaction engine knows two things: First, what functionality you want to achieve and, second, what hardware constraints you need to consider: number of qubits, depth of circuit, etc. So, you get two things: a synthesis of a quantum circuit from a high-level model, and an excellent optimization because the model knows the hardware constraints as well as the high-level requirements."

Functionality and Integration

Many users worry that each quantum company that comes along will require a steep learning curve, with more technological integration and additional languages to learn.

That's not an issue when users choose Classiq.

Classiq's platform is designed to match the client's quantum stack. The platform sits on top of popular programming languages such as Cirq, Qiskit, Braket and Q#. It works seamlessly with all quantum programming languages and with any universal gate-based quantum computer.

Customer, Investor Interest

Classiq continues to garner attention from customers and investors alike.

Enterprise quantum teams that are interested in developing applications or algorithms for quantum computers are choosing Classiq. The company is also developing ties with academia. Additionally, it has deep partnerships with the leading hardware providers.

Since its inception in late 2019, the company secured a total of about 18 million in funding from leaders in venture capital, including Team8 and Wing Venture Capital, Entrée Capital, OurCrowd, and IN Venture, the corporate venture arm of Sumitomo Corp.

63. A CLASSIQ SOLUTION launches new Center for Quantum Science and Engineering

by Matt Swayne
https://thequantumdaily.com/2021/09/01/epfl-launches-new-center-for-quantum-science-and-engineering/

Officials from Switzerland-based École Polytechnique Fédérale de Lausanne (EPFL) announced the creation of a center for Quantum Science and Engineering, which aims to be a global research center for the quantum era.

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

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

Major technological advancements

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

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

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

Two main research areas

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

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

A priority on education and research partnerships

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

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

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

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

