Crypto News

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

June 1, 2021

Contents

May 2021

31 May 2021

1 Declassified Cold War code-breaking manual has lessons for solving 'impossible' puzzles

by Richard Bean

https://theconversation.com/declassified-cold-war-code-breaking-manual-has-lessons-for-solving-impossible-puzzles-161595

The United States National Security Agency – the country's premier signals intelligence organisation – recently declassified a Cold War-era document about code-breaking.

The 1977 book, written by cryptologist Lambros Callimahos, is the last in a trilogy called **Military Cryptanalytics**. It's significant in the history of cryptography, as it explains how to break all types of codes, including military codes, or puzzles – which are created solely for the purpose of a challenge.

The first two parts of the trilogy were published publicly in the 1980s and covered solving well-known types of classical cipher.

But in 1992, the US Justice Department claimed releasing the third book could harm national security by revealing the NSA's "code-breaking prowess". It was finally released in December last year.

Lessons for code-breakers

A key part of Callimahos's book is a chapter titled Principles of Cryptodiagnosis, which describes a systematic three-step approach to solving a message encrypted using an unknown method.

An intelligence agency might intercept thousands of messages made in a target country's ciphers, in which case they already know the method. But if they encounter something new, they must first and foremost figure out the encryption method, or risk wasting time.

As Callimahos details in his chapter, the code-breaker must begin with all the necessary data. This includes the ciphertext (the enciphered text hiding the real message), any known underlying plaintext (text from before the encryption was applied), as well as important contextual information.

For puzzles, part of the plaintext may be given to help the solver. With confidential military messages, the solver may suspect certain words have been encoded into the ciphertext, based on past knowledge. For example, there may be key terms such as "message begins", "message ends" or "secret", or specific names, places or addresses.

The code-breaker then arranges and rearranges the data to find non-random characteristics. After this, they can recognise and explain these characteristics. In other words, they've found the cipher method.

Applying these steps is an example of "Bayesian inference". The code-breaker considers the weight of evidence and guesses the likely cause of an observed effect.

The Zodiac and Kryptos ciphers

Last year, the famous 1969 Zodiac killer cipher, known as **Z340**, was solved by an international team of code-breakers after 51 years. The team carefully and systematically developed a list of observations over many years.

Using a process called Monte Carlo sampling, they tested whether the patterns observed in the ciphertext were random or not. Together with a detailed knowledge of the context of the cipher and a solution for a previous cipher by the Zodiac killer, they correctly guessed the encryption method used.

One of the Zodiac cipher solvers, David Oranchak, said in his opinion it was "at about a seven or eight out of ten in difficulty to decipher".

Similarly, US artist Jim Sanborn's famous Kryptos sculpture, located at the Central Intelligence Agency, has long confounded attempts to unlock its code. It contains four encrypted passages to challenge the agency's employees. The final passage, known as K4, remains unsolved after 30 years.

When Kryptos's code designer Ed Scheidt was asked to rate the cipher's difficulty, he estimated it as being around a nine out of ten on the same scale. He said his intention was for it to be solved in five, seven or maybe ten years.

So what has made K4 so difficult? For one, with only 97 letters the passage is very short, meaning less data and fewer clues. The enciphering method used to create it is unknown, and there's little context as to how it may have been enciphered.

One classic book on mathematical problem solving, How to Solve It by George Pólya, suggests a general principle for solving any problem is to refer to a similar problem that has already been solved. This principle applies in the historical puzzle world, too.

However, Scheidt also noted there was a "change in the methodology" as the Kryptos message progressed – done intentionally to make it increasingly difficult.

It could also be that Sanborn accidentally introduced an error in K4 during the construction of the Kryptos sculpture, which would mean solvers are wasting their time. Making a mistake during enciphering can render a puzzle impossible to solve. In such cases, the creator should admit this to prospective code-breakers.

Lessons for code-makers

Looking at a puzzle from the code-maker's perspective is important. A skilled code-maker should leave at least some non-random patterns in the cipher, so as to not make their puzzle impossible.

Imagine you've created a puzzle, but after many years your intended audience has failed to solve it. If you still want it solved, you have to start releasing clues. Some puzzles, such as the 1979 book Masquerade and the Decipher Puzzles, were only solved after clues were released.

However, if nobody has solved your puzzle even after you release many clues, then the code is simply too tough to crack.

Cryptographer Helen Fouché Gaines wrote about this in her 1939 book. The creator of such a puzzle, she said, "fails to submit material in proportion to the amount of complication he has introduced".

This means you may have to eventually reveal the method you used. One example is a complex algorithm known as Chaocipher. While Chaocipher messages were designed to be highly difficult, they're virtually impossible to decipher without knowing the method.

A 2007 NSA presentation about Kryptos mentions how "dozens" of agency staff have failed to solve K4. But as more historical texts become declassified and our computational, storage and networking capacity grows, perhaps one day an amateur code-breaker – and not an agent of the NSA – will crack the elusive passage.

30 May 2021

2 Converting quantum promises into commercial realities

by Susan Curtis

https://physicsworld.com/a/converting-quantum-promises-into-commercial-realities/

We've all heard about the promise of quantum technologies to transform business and industry, whether it be for more secure communications networks or vastly more powerful computation. But what is needed to translate experimental quantum research into commercial success, and when can we expect it to happen?

According to speakers at the inaugural Quantum West conference, the transition from lab-based R&D towards market-ready solutions is already under way. While the headline-grabbing applications of quantum computing and the quantum Internet remain a longer-term bet, prototypes and products are already appearing in other areas of quantum technologies. One example is atomic clocks. Originally developed by the research community to provide more precise timing standards, the focus is now on re-engineering compact versions for use in high-speed mobile communications, synchronizing financial transactions, and other situations where accurate and resilient timekeeping offers a business advantage.

Applications for quantum sensors are also emerging. One notable example presented during the conference is a gravity sensor developed by Muquans, a French spin-off. Based on a Newtonian free-fall experiment in which a cloud of rubidium atoms cooled close to absolute zero is used as the test mass, Muquans' system integrates all the key components into a single unit that is robust and reliable enough to be deployed in the field for geophysical monitoring – including on the slopes of Mount Etna.

"I sometimes hear the question about what will be the first real-life application of quantum technologies," Muquans chief executive Bruno Desruelle told the Quantum West audience. "Well, there are already some quantum instruments that are in service now. We have built more than 10 units and we really believe that quantum technology offers a very interesting competitive advantage for gravity measurements."

While the Muquans instrument is aimed mainly at the scientific community, other sensors are being developed for a mass market. As an example, the UK start-up QLM has demonstrated a gas sensor that exploits photon quantum statistics to detect methane emissions. Such a sensor could replace the manual sniffer tests currently used in oil and gas exploration to spot leaks of this greenhouse gas, and QLM chief executive Murray Reed says the company is set to produce handheld units costing less than £1000 within the next few months. The same technology could also be used to monitor emissions of carbon dioxide.

Gateway to growth

The idea that early implementations of quantum systems for specific applications will pave the way for more ambitious commercial development is at the heart of the UK's National Quantum Technology Programme (NQTP). In his keynote address, Peter Knight, who serves on the NQTP advisory board, described its approach: "We identified a kind of funnel of what we're able to do in the very long term – for example, in quantum computing – and in the near term where we can pull out commercial and strategic value en route to achieving that long-term goal."

The programme, which was among the first government-sponsored initiatives to recognize and encourage commercial opportunities for quantum technologies, identified four key areas where quantum technologies

are likely to play an important role: sensing and timing, imaging, communications, and simulation and computing. For each area, it mapped out the commercial outcomes that could be achieved for each one over different timescales. In quantum communications, for example, a demonstrator project has already shown that quantum key distribution can be deployed in a standard fibre network, while ongoing NQTP-funded research focuses on developing quantum-resistant algorithms that will be needed to prevent attacks from next-generation quantum computers.

Matt Langione, a partner at the technology analytics firm Boston Consulting Group (BCG), delved deeper into the likely evolution of quantum computing, and its resulting market value, over the next 20 years. BCG's analysts compared the business opportunities that more computational power would bring with the hardware and software innovations needed to deliver it – whether through improvements to classical computation or the introduction of quantum-powered solutions.

Within the next three to five years, BCG's analysis suggests that early quantum processors with fewer than 1000 qubits, capable of tasks such as error mitigation and data compression, could deliver commercial value in four industry sectors: finance, pharmaceuticals, materials, and computational fluid dynamics simulations used in the automotive and aerospace industries. In this initial phase, Langione believes that the financial benefit for those four industries could reach a few billion dollars.

Further ahead, more sophisticated quantum computers – ones that exploit some level of error correction – will lead to a phase that Langione describes as offering a "broad quantum advantage". Such fault-tolerant quantum computers are expected to emerge in a decade or so, and could be used in simulations that speed up materials design and reduce risk in financial trading. In the process, they might boost the overall commercial benefit to $25 – 50bn.

Beyond that, from about 2030, quantum computers with full-scale fault tolerance could solve the kind of problems that would completely transform the commercial outcomes from these four industries – for example by enabling the discovery of completely new drugs and materials, or allowing banks to make the most efficient use of their capital. At that point, Langione predicts that the market value generated by quantum computers would reach hundreds of billions of dollars.

Engineering a quantum future

Such views may seem optimistic, particularly when current research efforts focus on scaling up quantum processors from mere tens of qubits to the hundreds and thousands required to build fault-tolerant quantum computers. Indeed, a major emphasis of the talks at Quantum West was the urgent need to engineer practical and scalable systems for operating such complex quantum systems. Underlining the scale of the challenge was Google's Eric Ostby, who revealed that at least 8000 additional components are currently needed to control and read out the 54 qubits in the company's latest quantum chip.

More generally, engineering any practical quantum system will mean replacing today's intricate experimental set-ups with robust and reliable plug-and-play units. Key to the success of the Muquans gravimeter, for example, is a bespoke laser technology that replaces optical components carefully arranged on an optical table with a solid-state frequency-doubling architecture that offers greater stability as well as easy integration with standard telecoms components.

This being Photonics West, many of the speakers focused on the crucial importance of photonics technologies for quantum applications. Lasers, for example, are widely used to manipulate quantum states, and over the last few years many devices have emerged with the narrow linewidths and wide tunability needed for quantum experiments. Even so, Scott Davis, chief executive of laser manufacturer Vescent

Photonics, was candid about the shortfalls of the current generation of these devices. “There’s a gap between current laser reality and what the quantum system engineers want,” he said. “They are looking for something like a telecom package that’s cheap and fully integrated, while today’s devices only operate at certain wavelengths and are still really only designed for use in the lab.”

Part of the problem for companies such as Vescent is that there is no clear roadmap to guide their product development efforts. With this in mind, the Quantum Economic Development Consortium (QED-C), an organization that aims to support the growth of the US quantum industry, organized a workshop in September 2020 to discuss the future photonics requirements for quantum applications.

“One of the big takeaways is that the path forward for lasers for quantum is not so clear,” noted Davis, who chaired the workshop. “It’s a complicated space right now, with lots of different applications calling for different wavelengths and laser properties.” As a result, QED-C has launched an initiative to identify the technology and market intersections that should be tackled first.

Meanwhile, Davis is convinced that the best way to reduce the current market uncertainty is to get involved with academic research projects. Working in partnership with quantum scientists helps laser manufacturers to design devices that meet the specific technical requirements, from which they can engineer more integrated products that can be sold to equipment manufacturers. This has allowed Vescent to create, for example, an integrated laser-based system that has already been deployed in quantum sensors and atomic clocks.

Many other speakers stressed the need for strong collaboration between industry, academia and government programmes to drive early commercialization efforts. This approach has already been formalized in some parts of the world, including the UK. Knight described the NQTP as building a “quantum alliance” between academic research groups (which focus on creating scientific knowledge), large and small companies (which can identify market opportunities and build practical solutions), and government (which functions as a sponsor and early adopter of quantum technologies). A measure of its success, Knight said, is that in a recent funding round for larger projects, 63 companies were involved in bids for the available £84m, and these businesses had themselves raised an additional £109m for quantum technology development over the last two years. “The appetite for working on this and translating the technology into the market is really there,” he said. “Working together we can do so much more than working apart.”

3 The SolarWinds hackers aren’t back – they never went away

by lily hay newman

https://arstechnica.com/gadgets/2021/05/the-solarwinds-hackers-arent-back-they-never-went-away/

The Russian hackers who breached SolarWinds IT management software to compromise a slew of United States government agencies and businesses are back in the limelight. Microsoft said on Thursday that the same “Nobelium” spy group has built out an aggressive phishing campaign since January of this year and ramped it up significantly this week, targeting roughly 3,000 individuals at more than 150 organizations in 24 countries.

The revelation caused a stir, highlighting as it did Russia’s ongoing and inveterate digital espionage campaigns. But it should be no shock at all that Russia in general, and the SolarWinds hackers in particular, have continued to spy even after the US imposed retaliatory sanctions in April. And relative to SolarWinds,

a phishing campaign seems downright ordinary.

“I don’t think it’s an escalation, I think it’s business as usual,” says John Hultquist, vice president of intelligence analysis at the security firm FireEye, which first discovered the SolarWinds intrusions. “I don’t think they’re deterred and I don’t think they’re likely to be deterred.”

Russia’s latest campaign is certainly worth calling out. Nobelium compromised legitimate accounts from the bulk email service Constant Contact, including that of the United States Agency for International Development. From there the hackers, reportedly members of Russia’s SVR foreign intelligence agency, could send out specially crafted spear-phishing emails that genuinely came from the email accounts of the organization they were impersonating. The emails included legitimate links that then redirected to malicious Nobelium infrastructure and installed malware to take control of target devices.

While the number of targets seems large, and USAID works with plenty of people in sensitive positions, the actual impact may not be quite as severe as it first sounds. While Microsoft acknowledges that some messages may have gotten through, the company says that automated spam systems blocked many of the phishing messages. Microsoft corporate vice president for customer security and trust Tom Burt wrote in a blog post on Thursday that the company views the activity as “sophisticated” and that Nobelium evolved and refined its strategy for the campaign for months leading up to this week’s targeting.

“It is likely that these observations represent changes in the actor’s tradecraft and possible experimentation following widespread disclosures of previous incidents,” Burt wrote. In other words, this could be a pivot after their SolarWinds cover was blown.

But the tactics in this latest phishing campaign also reflect Nobelium’s general practice of establishing access on one system or account and then using it to gain access to others and leapfrog to numerous targets. It’s a spy agency; this is what it does as a matter of course.

“If this happened pre-SolarWinds we wouldn’t have thought anything about it. It’s only the context of SolarWinds that makes us see it differently,” says Jason Healey, a former Bush White House staffer and current cyberconflict researcher at Columbia University. “Let’s say this incident happens in 2019 or 2020, I don’t think anyone is going to blink an eye at this.”

As Microsoft points out, there’s also nothing unexpected about Russian spies, and Nobelium in particular, targeting government agencies, USAID in particular, NGOs, think tanks, research groups, or military and IT service contractors.

“NGOs and DC think tanks have been high-value soft targets for decades,” says one former Department of Homeland Security cybersecurity consultant. “And it’s an open secret in the incident response world that USAID and the State Department are a mess of unaccountable, subcontracted IT networks and infrastructure. In the past, some of those systems were compromised for years.”

Especially compared to the scope and sophistication of the SolarWinds breach, a widespread phishing campaign feels almost like a downshift. It’s also important to remember that the impacts of SolarWinds remain ongoing; even after months of publicity about the incident, it’s likely that Nobelium still haunts at least some of the systems it compromised during that effort.

“I’m sure that they’ve still got accesses in some places from the SolarWinds campaign,” FireEye’s Hultquist says. “The main thrust of the activity has been diminished, but they’re very likely lingering on in several places.”

Which is just the reality of digital espionage. It doesn’t stop and start based on public shaming. Nobelium’s activity is certainly unwelcome, but it doesn’t in itself portend some great escalation.

27 May 2021

4 Cambridge Quantum Develops Algorithm to Accelerate Monte Carlo Integration on Quantum Computers

https://cambridgequantum.com/cambridge-quantum-develops-algorithm-to-accelerate-monte-carlo-integration-on-quantum-computers/

Cambridge Quantum Computing (CQC) today announced the discovery of a new algorithm that accelerates quantum Monte Carlo integration – shortening the time to quantum advantage and confirming the critical importance of quantum computing to the finance industry in particular.

Monte Carlo integration – the process of numerically estimating the mean of a probability distribution by averaging samples – is used in financial risk analysis, drug development, supply chain logistics and throughout other business and scientific applications, but often requires many hours of continuous computation by today's systems to complete. It is a critical aspect of the computational machinery underpinning the modern world.

CQC have solved the problem with an algorithm detailed in a released pre-print of a paper by Senior Research Scientist, Steven Herbert, showing how historic challenges are eliminated, and the full quadratic quantum advantage is obtained.

"This new algorithm is a historic advance which expands quantum Monte Carlo integration and will have applications both during and beyond the NISQ era," Herbert said. "We are now capable of achieving what was previously only a theoretical quantum speedup. That's something that none of the existing quantum Monte Carlo integration (QMCI) algorithms can do without substantial overhead that renders current methods unusable."

Ilyas Khan, CEO of Cambridge Quantum Computing, "This is an impressive breakthrough by the scientists at CQC that will be of tremendous value to the financial sector as well as many other industries and is just the latest in a continuing streak of innovations that confirm our world leading position in quantum computing."

26 May 2021

5 A Gardener's Perspective On Cryptographic Management

by Mike Brown

https://www.forbes.com/sites/forbestechcouncil/2021/05/26/a-gardeners-perspective-on-cryptographic-management/?sh=3b827d2c5c58&utm_medium=email&_hsmi=129917135&_hsenc=p2ANqtz-_bgQtZLlBQPsgHOQVb_e5OVbKZTyOZ_wjueJikPhVXZOCB_Oey6KABYQwL7GGVqPZuLaLiTBKlEMAD7PoltM11gKW4jw&utm_content=129917135&utm_source=hs_email

What do cryptographic management and a vegetable garden have in common? From a gardener's perspective, quite a bit. It is now spring, and the gardeners among us have already started taking action with garden maintenance, preparation and planning to ensure the success of this year's harvest.

As any gardener knows, a successful garden requires work throughout the year. In the autumn, you tidy up last year's scraggly plants and mulch. In the winter, you take an inventory of your seeds and maybe

buy new ones. In the spring, you get everything in the ground (once the frost is gone!), add compost and water, and hope for lots of sunshine. In the summer, you water, fertilize and weed the garden – and start enjoying the harvest.

Gardening, much like an organization's security, requires constant vigilance. Maybe you had a bad patch of potatoes and now you have mold. Maybe rabbits moved in and you need to put up fencing to protect the lettuce. Or maybe you have snails and you need to lure them away. As a gardener, you need to know what plants you have, how to care for them and how to protect them against threats.

Threats change over time (weather, pests, soil, location), so you are always revisiting and revising the steps you need to take. And sometimes, you need to dig it all up and start fresh. Gardens require lifecycle management to maximize the harvest.

The Crypto-Gardener: Always Evolving

Cryptography has become a critical component of ensuring a strong enterprise security posture. In the past, we trusted our cryptography without question, and unless you were in a heavily regulated industry, such as banking (where compliance is essential), it didn't require much attention or maintenance. Today, almost every application and IT system that you interact with on a daily basis contains cryptography; it's found throughout all the various layers of an organization's infrastructure, whether on-premises or cloud-based.

Throughout your infrastructure, do you know which cryptography is healthy, which is weak and which is completely unacceptable? Or do you have very outdated cryptography that is difficult to fix, so you just accept the risk and give it a pass year after year? There's also the threat from quantum computers on the horizon, which NIST is addressing with a new set of quantum-safe cryptography standards that enterprises will need to migrate to in the next two to four years. Whether it's the quantum computing threat or some other future threat, "There are real dangers to inaction," warn researchers with Deloitte's Center for Government Insights.

Managing Your Cryptographic Garden

Modern cryptography management requires an ongoing, strategic focus. Like a weed in a garden, you sometimes find cryptography where you don't expect it. It is essential to keep an up-to-date inventory of what cryptography is in your environment and what applications and systems are using it. That way, you can regularly review and identify where your deficiencies are and put plans in place to address them. In cryptographic management, a crypto-gardener undergoes these four phases:

(i) **Discovery:** Create a library of cryptographic assets.

(ii) **Triage:** Analyze and prioritize which risks need to be fixed and in which order.

(iii) **Remediation:** Fix what you can. Patch what is available and make sure to track what you can't.

(iv) **Repeat:** Why is there such a great need to know about your cryptographic assets? It's about discovering what you may not already know, such as a threat that can be mitigated. No one likes an unknown (like that pesky rabbit sneaking in to eat your baby lettuce shoots). Additionally, organizations need to consider their supply chains, third parties, regulators and compliance requirements.

With cryptography at the core of every secure data transmission and transaction, an organization's cryptography requires constant management. A well-managed cryptographic infrastructure and a well-managed garden both require dedication, awareness, pro-activeness, care and ongoing management. British horticulturist Gertrude Jekyll once said, "A garden is a grand teacher. It teaches patience and careful watchfulness." Here's to sowing the seeds and reaping the benefits of your "garden."

25 May 2021

6 Keysight Technologies Acquires Quantum Benchmark

by santa rosa

https://www.keysight.com/in/en/about/newsroom/news-releases/2021/0525-nr21083-keysight-technologies-acquires-quantum-benchmark.html

Keysight Technologies, Inc., a leading technology company that delivers advanced design and validation solutions to help accelerate innovation to connect and secure the world, announced today it has acquired Quantum Benchmark, a leader in error diagnostics, error suppression and performance validation software for quantum computing.

Based in Kitchener, Ontario, Canada, Quantum Benchmark was a privately held company backed by venture funds VanEdge Capital and Quantonation. Quantum Benchmark provides software solutions for improving and validating quantum computing hardware capabilities by identifying and overcoming the unique error challenges required for high-impact quantum computing.

"Joining forces with Keysight is a strategic and timely opportunity to accelerate the development and delivery of our industry-leading solutions," said Joseph Emerson, Ph.D., Quantum Benchmark CEO, Founder and Chief Scientist. "Together, we bring the world closer to achieving the break-through applications of quantum computing including the design of energy-efficient materials, the acceleration of drug discovery, the promise of quantum machine learning, and so much more."

Quantum computing is an emerging technology that is expected to simulate real-world systems and tackle problems that are otherwise intractable with conventional computing. Quantum systems use qubits (quantum bits) to process data. As quantum computing technology evolves, the ability of quantum computers to perform meaningful computations is determined by the number of qubits, as well as by the quality of those qubits. Performance-limiting errors invariably arise in qubit hardware and present the key challenge to large-scale quantum computing. Quantum Benchmark's technology improves the quality of the qubits across all quantum hardware platforms and delivers solutions at both ends of the quantum market. It helps quantum hardware makers design better qubits and helps quantum end-users stabilize the performance of those qubits for their specific use-cases.

Quantum Benchmark's technology is based on years of research by several of the world's leading experts in quantum computing at the University of Waterloo's Institute for Quantum Computing. The acquisition of Quantum Benchmark supports Keysight's goal to deliver a comprehensive quantum portfolio addressing customer needs across the physical, protocol, and application layers. Quantum Benchmark represents Keysight's third acquisition in the quantum space after Signadyne in 2016 and Labber Quantum in 2019.

"As the quantum ecosystem continues to form, Keysight is committed to providing customers with a full suite of solutions for the overall quantum stack. We are pleased to announce the addition of Quantum Benchmark to our portfolio, providing unique capabilities for solving complex qubit error and validation

challenges," said Kailash Narayanan, president of Commercial Communications at Keysight. "The talented Quantum Benchmark team will be a valuable addition to Keysight and will further our mission to accelerate innovation to connect and secure the world."

7 Hack, disinform, deny: Russia's cybersecurity strategy

https://www.moneycontrol.com/news/world/hack-disinform-deny-russias-cybersecurity-strategy-6935391.html

Over the years, Moscow has faced numerous allegations of cyberattacks that resulted in multiple sanctions and the expulsion of its diplomats. The term "hacker" has almost become synonymous with Russia.

From "troll factories" to hackers allegedly controlled by the country's security services, here is an overview of the world of Russian cybercrimes:

- **Skills**

  Russia has for decades been a breeding ground for computer experts. During Soviet times, the government pushed for advances in science and technology, and – with the appearance of the first computers – in programming.

  With the fall of the USSR in 1991, some of the talented but underpaid programmers turned to cybercrime, soon making Russians notorious for credit card thefts around the world.

  "In the 90s, the environment fermented, with a culture of resourcefulness and a tendency to circumvent the rules," said Kevin Limonier, of the French Institute of Geopolitics.

- **Army and security services**

  Experts say that in its persisting stand-off with the West, Russia heavily relies on its cyber and information warfare capabilities.

  Several notorious hacking groups are suspected of working for the country's security services, and the Russian defence ministry established its own "cyber units" in 2012.

  The first large-scale attack attributed to Russia goes back to 2007, when the Baltic state of Estonia faced a wave of cyberattacks on its newspapers, banks and government ministries.

  The United States says that hackers of Russia's military intelligence (GRU) sought to manipulate the 2016 presidential election by hacking into the Democratic National Committee and the Hillary Clinton campaign.

  The most famous cyber-espionage group involved in dozens of cases is known as Fancy Bear or APT28. It is believed to be sponsored by the Russian government.

  According to Washington, the attack targeting US software developer SolarWinds was carried out by the SVR, Russia's foreign intelligence service, and compromised government agencies and hundreds of private companies.

- **Information and sabotage**

  "Cyberattacks carried out by Russian secret services are part of multi-year international operations that are aimed at obtaining strategic information," German intelligence said in 2016, referring to espionage and sabotage operations.

The list of alleged Russian attacks is long: a hacking attack on the German parliament in 2015; targeting Ukrainian artillery units between 2014 and 2016; hacking of a French television network in 2015; meddling in US elections in 2016 and 2020, and targeting coronavirus vaccine research institutes in the West in 2020.

Experts say that attacks are becoming ever more sophisticated.

"The level of Russian cyberattacks is growing compared to three or four years ago," said intelligence expert Andrei Soldatov.

"We know about the operations that have been uncovered but a lot still remains effective."

- **Disinformation**

  Russia has also been accused of carrying out large-scale disinformation campaigns in order to sway democratic processes in the West and fuel social discord online.

  The country is believed to be operating online "troll factories" that concoct fake viral information in an attempt to influence internet users.

  The accusations have been directed against both state media including RT (former Russia Today) and Kremlin allies such as Yevgeny Prigozhin, a businessman suspected of being at the origins of "troll factories" in Russia and Africa.

  Washington has accused the ally of President Vladimir Putin of financing the Internet Research Agency, a Saint Petersburg-based company that sought to influence the US electorate in 2016.

- **Denial**

  Aware that the nature of cyberattacks makes their origins difficult to trace, the Kremlin has always denied any involvement and accused the West of waging a disinformation war on Russia.

  Russia has also repeatedly pledged its desire to cooperate in the cyber sphere.

  In the run-up to the 2020 US presidential elections, Putin proposed a pact of electoral non-interference and a global agreement against the misuse of communication technologies.

  The proposal was left without response.

  Soldatov said that Russia might be using hacking attacks to force the West to cooperate.

  He did not rule out that, faced with the Russian threat and for want of a better alternative, "police in Europe and the United States might like to return to cooperating with Russia on cybersecurity".

24 May 2021

8 Viewing Enterprise Cryptography In A New Light: Traversing A Fragmented Environment

by Professor Yehuda Lindell

https://informationsecuritybuzz.com/articles/viewing-enterprise-cryptography-in-a-new-light-traversing-a-fragmented-environment/

Cryptography has taken a tumultuous journey over the past 20 years. As the digital world has evolved, its role in protecting the modern enterprise has become more crucial than ever. Cyber attackers now lie in

wait for businesses, and there is no perimeter strong enough to keep them out. As a result, organisations are deploying zero-trust solutions, ensuring security even in the case of a breach. The modern security challenge has been made even more complicated by the move to remote working, BYOD policies and increasingly hybrid scenarios involving an organization's data centers and multiple clouds. Cryptography is now increasingly needed in the modern environment of remote management, but the pace needed in implementing it enterprise-wide is a challenge all in itself.

At the core of this is the fact that the cryptographic space is currently highly fragmented, with numerous solutions inherently utilizing the technology. There are many ways to authenticate identity, such as passwords, OTP and smartcards, plus numerous cryptographic methods for encrypting databases, VMs, storage and more across different clouds and data centers. To add further complexity, cryptographic signatures are also required for documents, transactions and code. Multiple point and siloed solutions can result in reduced visibility, agility, and flexibility, not to mention the strain on management with high costs involved in the deployment in different environments.

Determining a new approach

Managing and deploying cryptographic solutions in the modern age requires a new approach, with multiple layers to consider:

- **Making the shift to hybrid hardware and software:** Hardware solutions have traditionally powered legacy key protection. In today's environments where everything is virtualized and managed remotely, and enterprises are moving to cloud deployments, pure hardware solutions constitute a significant obstacle. As a result, software solutions for key protection with strong guarantees are needed to replace and complement existing hardware.
- **Transforming from siloed to unified key management:** While legacy key protection and management has been comprised of different solutions, a unified approach with one platform that can support all cryptographic solutions in any environment is needed today.
- **Ensuring integrated key management and key protection:** Legacy key protection provides only simplistic management and dedicated key management solutions are often not integrated with key protection. A unified platform providing integrated key protection and management is required.
- **Key misuse prevention:** Legacy key protection solutions address the problem of key theft only. Today, key misuse must be addressed as an integral part of key protection.
- **Adopting an agile infrastructure:** Rigidity plagues legacy key protection and management solutions. Cryptography standards are continually changing; updates must be rolled out quickly and new threats need to be considered and resolved. Today's cryptographic infrastructure needs to support agility.
- **Speeding up deployment:** Legacy cryptographic solutions that relied solely on hardware were ultimately slow in deployment. Today, enterprise security teams must offer on-demand cryptographic services internally in order to quickly support business needs.

Evidently, the fragmented legacy cryptographic infrastructure of the 1990s does not support modern business needs and is in desperate need of modernization.

Clearing a path

To address these challenges, firstly, modern solutions are needed that are based on openness and transparency in collaborative environments. Second, modern computing environments need modern software. Third, a new technological approach is required to deliver a software key store with proven security guarantees to complement legacy hardware and support new security requirements. Legacy solutions involved building a fortress around the device that held key material and prevented any attacker from breaching that machine. In today's zero-trust environments, this is problematic when it comes to software-only solutions.

A different approach is to ensure that cryptographic keys are never kept in one single place at any particular time, forcing a cyber attacker to simultaneously breach several machines in order to gather information. That way there would be no single point of security failure, and strong separations between the different machines would make it extremely hard to breach.

The question however still remains; How can one cryptographic operation such as decryption or signing be carried out without holding the key? Fortunately, a methodology called **Secure Multiparty Computation (MPC)**, also known as threshold cryptography, can do exactly this. Using MPC, the secret key is generated in two or more parts called shares, so that all shares are needed to get any information about the key. These different shares reside on different servers and devices, so that an attacker has to breach them all to steal the key.

MPC protocols enable different machines to obtain the result of the cryptographic operation, without combining any of the shares or revealing any sensitive information about the key. This means the key remains fully protected, even while in use. MPC protocols have mathematical proofs of security, guaranteeing that an attacker who cannot breach all machines is unable to learn anything about the key, even if they know the protocols used. Although anti-intuitive, when using MPC, the key is never whole in any single place, not whilst in use or while the code is generated.

Adopting a unified solution

In moving to a unified approach to key storage, organizations can ensure transformation in their existing fragmented infrastructure, allowing for improvements in efficiency, security, user experience and cost savings, while providing the necessary infrastructure for all cryptographic requirements in the business. Virtualizing cryptography allows for consistency with how other software works within the organization, ensuring scalability in cloud or on-premise environments and enabling agility in a cost-effective manner. Most critically, however, such solutions allow key orchestration across the enterprise and management of all cryptographic solutions from one location, bringing cryptography into a new technological phase.

9 Explore today's quantum systems with Azure Quantum

by Julie Love

https://cloudblogs.microsoft.com/quantum/2021/05/24/explore-todays-quantum-systems-with-azure-quantum/

Companies and application partners are opening up new avenues of research using Azure Quantum to experiment with building and running quantum algorithms on leading quantum hardware from Honeywell Quantum Solutions and IonQ.

One of the challenges in quantum computing is understanding where the practical impact will be as hardware capabilities mature. At this week's Microsoft Build, Microsoft's Mariia Mykhailova explains the important role our quantum software development tools play in researching and testing quantum algorithms on quantum hardware through Azure Quantum. To help developers build skills in this critical area, Mariia breaks down the hybrid quantum software development workflow into steps, explaining each step and related tools in detail, many of which a classical developer will find familiar.

At Microsoft Build, Brian Neyenhuis from Honeywell Quantum Systems will also share how Japan's largest oil company ENEOS and Microsoft Quantum Network partner QunaSys use Honeywell's trapped-ion system for practical quantum chemistry research. Vibration spectrums are used to identify chemical compounds, understand equilibrium and transitional structures in chemical reactions, and understand thermodynamic quantities like free energy. The experiment simulates the molecular vibration modes of water and methanol, showing agreement between the quantum simulation and the known values. These types of experiments performed on systems available today help determine what future scaled-up systems can accomplish with bigger problems. We can take this knowledge forward as more scalable quantum hardware becomes available. Be sure to view the full Microsoft Build session, Develop and Run Quantum Algorithms on Today's Systems with Azure Quantum.

Azure Quantum provides multiple paths to explore and build solutions with quantum technologies – both quantum-inspired optimization solutions running on classical hardware and quantum solutions running on today's quantum hardware. Azure Quantum provides powerful tools, leading quantum hardware, learning resources, and a vibrant ecosystem for experimentation and quantum software development. You can use the familiar and trusted Azure platform to learn how to develop quantum algorithms and how to program and run them on real hardware from multiple providers. Developers, application partners, and businesses around the world are experimenting with Azure Quantum to access the best available quantum computing capabilities today.

Get started today and learn about quantum development with Q#, QDK, and Azure Quantum at the Azure Quantum Developer Workshop 3 on June 30, 2021.

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

by Stephen Shankland

https://www.cnet.com/news/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/?

Quantum computers, if they mature enough, will be able to crack much of today's encryption. That'll lay bare private communications, company data and military secrets.

Today's quantum computers are far too primitive to do so. But data surreptitiously gathered now could still be sensitive when more powerful quantum computers come online in a few years.

The computing industry is well aware of this potential vulnerability. Some companies have embarked on an effort to create, test and adopt new encryption algorithms impervious to quantum computers. Some of those companies, including IBM and Thales, have already begun offering products protected by what's called post-quantum cryptography.

Quantum-safe encryption will come into your life through upgraded laptops, phones, web browsers

and other products. But most of the burden for quantum-safe encryption rests on the shoulders of businesses, governments and cloud computing services that must design and install the technology. It's an extraordinarily complex change that's on par with fixing Y2K bugs or upgrading internet communications from IPv4 to IPv6.

It's a colossal effort, but it has to be done. Not only are today's communications vulnerable, but quantum computers later could crack the digital signatures that ensure the integrity of updates to apps, browsers, operating systems and other software, opening a path for malware.

Quantum computing is the darling of the industry, and it's attracted millions of dollars in investment. At this month's Google I/O developer conference, the search giant unveiled plans for a new quantum computing center that will employ hundreds of people with the goal of building a practical quantum computer by 2029. Other tech giants, such as Honeywell, IBM, Intel and Microsoft, are racing to build the first powerful quantum computers. So are IonQ, PsiQuantum, Xanadu, Silicon Quantum Computing and other startups.

Finding post-quantum crypto algorithms

The US National Institute of Standards and Technology is spearheading the global effort to find post-quantum cryptography algorithms that will be fast and trustworthy. It's winnowed 82 initial contributions down to a group of seven final candidates for two encryption tasks: exchanging digital keys and adding digital signatures.

"We expect toward the start of 2022 or so, we will select a small number of them to begin being standardized," Dustin Moody, a NIST mathematician working on the effort, said at an IBM cryptography meeting in March. "We hope to have the final version completely ready and published around 2024."

Though NIST oversees the work, researchers from business, academia and the government are participating through NIST's post-quantum cryptography mailing list and public PQC conferences. The open approach is important since encryption algorithms require deep scrutiny before we can trust them to protect our passwords, credit card numbers, financial records and other sensitive information.

When these machines will be able to crack conventional encryption is an open question. But the safe money suggests it won't take long.

John Graham-Cumming, chief technology officer of internet infrastructure company Cloudflare, said there's a lot of uncertainty: It could take five years before quantum computers can crack encryption or it could take 20. But already Cloudflare has tested post-quantum protections and plans to adopt them for internal operations this year.

Researchers at Intel and NTT Research and 451 Research analyst James Sanders reckon it will take on the order of a decade.

How urgent is fixing the problem?

"I'm not quite hair on fire," said Brian LaMacchia, who leads encryption work at Microsoft Research. "But I'm a little singed."

Harvest data now, crack it later

The urgency comes because today's encrypted data could be collected now and cracked later. Hackers or nations can record network data, for example, when internet routing problems send traffic across borders to China or other nations.

"If you want long-term security, it might even be too late," said Thomas Pöppelmann, a cryptography engineer at German chipmaker Infineon and co-creator of one of the PQC algorithm candidates.

NIST has a blunt assessment of the problem. When cyber adversaries have access to the power of quantum computing, our modern cryptographic systems based on public keys won't stand up to the test. "Nothing can be done to protect the confidentiality of encrypted material that was previously stored by an adversary," the agency says.

Public key cryptography is the foundation for much of today's encryption. It pairs two digital keys, one secret and one public, that together can be used to secure communications. For example, it's used to establish the security of connections between your web browser and your bank or between a company server and a remote backup system.

Shor's algorithm and cracking encryption

In 1994, Peter Shor, a professor at MIT, figured out that quantum computers could find the prime factors of numbers through a technique now named after him. Shor's algorithm was the spark that ignited quantum computing interest from companies, academics and intelligence agencies, says Seth Lloyd, another MIT professor and a pioneer of the field.

The resulting research is why major companies and well-funded startups are picking up the pace of their quantum computing progress. Quantum computer makers are building machines with more and more qubits – their fundamental data processing elements – while developing error correction techniques to keep them stable through longer calculations. Algorithms are speeding up quantum computer decryption, too.

Accelerating quantum computing progress

The quantum computing progress led cybersecurity firm Deepwatch to speed up its timetable for encryption cracking. Instead of taking 20 years, it could happen in 10 to 15 years, said Marissa "Reese" Wood, vice president of product and strategy.

For today's ubiquitous RSA encryption algorithm, a conventional computer would need about 300 trillion years to crack communications protected with a 2,048-bit digital key. But a quantum computer powered by 4,099 qubits would need just 10 seconds, Wood said.

For comparison, Google hopes to build a quantum computer in 2029 with 1,000 "logical" qubits – ones stable enough to perform a long calculation.

What to do about post-quantum encryption

The quantum transition is in many ways harder than some past encryption upgrades. One problem is that digital key sizes likely will be larger, requiring more memory to process them. Changing algorithms won't be a simple swap, especially for smart home devices and other products with limited computing horsepower.

Even before NIST picks its winners, companies can embrace "crypto agility" in today's computing infrastructure, ensuring their systems aren't reliant on a particular encryption technology. That's the advice of several experts, including Andersen Cheng, chief executive officer of Post-Quantum, a London-based company that helps customers deal with quantum cracking.

"People thought I was mad" when he co-founded Post-Quantum in 2009, Cheng said. "I don't think they're laughing anymore."

Experts also recommend a hybrid approach that double-protects data with both conventional and post-quantum security encryption. That lets system administrators embrace PQC sooner without worrying as much about weaknesses that could be found in relatively immature algorithms. Hybrid encryption is possible now, though most expect serious adoption of PQC to take place after NIST is done with its standardization work.

IBM already offers quantum-safe crypto in several cloud computing products today. "If you have secrets which need to remain secret 10 to 30 years from now, you should begin this migration sooner than later," said IBM Research cryptography researcher Vadim Lyubashevsky.

France-based Thales, which like IBM has a PQC algorithm in NIST's final round, has begun letting clients test the technology. That's important given its clout with finance and government customers.

Not an easy upgrade

Switching to quantum-safe encryption in slower-moving computing infrastructure is harder.

"Estonian voting cards have a signature algorithm that's physically burned into a chip," said Joël Alwen, chief cryptographer at secure communications company Wickr. "That's going to be a huge effort to change that."

Another tough fix will be computer systems that control power grids and military operations. They typically run for decades. But wherever there's sensitive data, post-quantum cryptography upgrades will happen, said Gartner analyst Martin Reynolds.

"In 20 years," Reynolds said, "everyone will be glad we did it."

11 Let's Talk Quantum – In Defense & Warfare

by Elets News Network

https://cio.eletsonline.com/article/lets-talk-quantum-in-defense-warfare/67778/

It has always been witnessed that the defense research organizations of various countries across the globe used to be in the forefront when it comes to adopting cutting-edge technologies. Of course, it was a question of survival and first-mover advantage during the two World Wars, but it continued to be a tradition even after that and countries continued to invest a lot in their technological endeavors in the field of defense research. It is also true that many of the technological innovations and breakthroughs we are enjoying today had happened in the defense research labs at one point and later extended to the industry and academia. So, a powerful quantum computing ecosystem is already in the wish list of the defense research departments of many countries. And why not, in this age of Cyber and Cyborg warfare, quantum computing can definitely play the role of a game changer. Experts believe that quantum computers could make a significant contribution to the future of military equipment & ammunition industries.

This article is NOT intended to showcase the dark side aspects of quantum computing, rather intension is to highlight the possible applications of this groundbreaking technology.

Defense scientists of many countries are taking a closer look at the impact that Quantum Computing, Quantum Communications and IoT will have on their national security and defense. It is believed that of

the two areas, Quantum Encryption and Quantum Sensors will have an enormous impact in this field in coming years. Use of quantum computers in communications that can revolutionize Underwater Warfare is of paramount importance in the defense world.

The Quantum Computation and Quantum Communication will also revolutionize “Defense Logistics”. Declining cycle times, increased awareness of the situation and more efficient communication are just some of the advantages that quantum computation or quantum communication will offer in the field of Defense Logistics.

Technologies like Artificial Intelligence, Virtual Reality, Augmented Reality and Blockchain are already in use to enhance defense capabilities. The future of warfare will be determined by new technologies such as Space based Internet Infrastructure/backbone and Quantum based Cryptography etc. While the use of quantum computing could mean that today’s widespread and critical encryption methods will become obsolete, the technology also promises a whole new generation of secure communications. We can expect the use of a quantum cryptography network and a significant increase in the number of fast & secure communication networks in coming years. Also, one of the most promising applications for quantum computing in military defense is “Lattice-Based” cryptography, which can provide algorithms that are safe against quantum attacks.

Also, accurate navigation that does not require GPS signals, is one of the most sought-after skills that would be supported by quantum computing technology.

Intelligence agencies around the world, in particular are investigating quantum computing for its possible use as a means of gathering and monitoring vital information. In the future, it could also be used for analysis and data mining and many such things that are very essential as part of intelligence gathering for the agencies. Such agencies in particular are fascinated by the potential of the quantum computing systems to develop secure communications and inertial navigation. Given these strategic applications, there is a strong interest in harnessing the power of quantum mechanics, and governments around the world are investing in this area to preserve and maintain strategic advantages.

Quantum Machine Learning algorithms are likely to be used for a wide range of applications such as GPS navigation and inertial navigation in GPS systems. The US Air Force, Marine & Lockheed Martin exploring it in the development of advanced navigation systems and advanced communications systems for the Navy and Marines.

That day is not far when many countries would like their defense departments to have access to the world’s most advanced quantum computing technology for many advantages and there has already been a huge investment done on Quantum research by many wealthy nations. USA, China and few other European countries are already ahead in the race and many others are in the process of developing their indigenous quantum computers. In India, Tata Institute of Fundamental Research is the pioneer in this field and trying to build a 3 Qubit Quantum Computer to demonstrate a unique design and architecture which is indigenously developed by the scientists of TIFR, once this model is successful, the scientists believe that scaling it to higher number of Qubits will not be so difficult. They also claim that this design an approach of building quantum processor many have many more advantages than the design & approach used in some of the existing quantum computers. Also, India Government recently declared more than eight thousand crores for quantum computing research which is a very good sign for a country like India.

21 May 2021

12 Quantum computing is here; Is a quantum PC next?

by Dan O'Shea

https://www.fierceelectronics.com/electronics/quantum-computing-s-here-a-quantum-pc-next

The Inside Quantum Technology Conference this week featured virtual panel of experts after virtual panel of experts laying out reasons why quantum computing is no longer a physicist's pipe dream, and instead is real and here and brimming with potential to fuel a variety of projects and applications across many industries.

Although, "real and here" for most of us means in the cloud. That's where many quantum computers, like IBM Quantum, exist today. Users, mostly researchers, students and other academic types, register to use cloud-based quantum computing resources. That's why much of the market value of quantum computing in the next few years will be derived from cloud access to quantum computing resources and not from computing hardware and software components, as Lawrence Gasman, conference founder and president of IQT Research said during the event.

That begs two questions: Will cloud-based quantum computing ever give way to on-premises quantum computing, and if that's possible, will we ever see such a thing as a quantum PC?

In a conference talk that he said attendees shouldn't take "too seriously, with an emphasis on 'too" Gasman speculated on those questions. There are three potential alternative methods for accessing quantum counting resources: the cloud model of today, the emerging notion of a quantum Internet and the possibility of a quantum desktops, that is to say rack mounted machines or table-sized units that could be used in data centers and similar environments.

The notion of a quantum internet was mentioned in passing by several conference panelists this week, and was the subject of a separate talk by Stephanie Wehner, roadmap leader of the quantum internet and network computing initiative at QuTech, who called the idea "something that sounds like a lofty goal, but is actually much more realistic." She said the industry is making progress on quantum networks that consist of end nodes that currently can transmit qubits between them along a fiber route with repeaters in place for extended transmissions. This could enable applications such as advanced optical clock synchronization across networks and the creation of quantum computing clusters capable of more powerful computations and use cases than we see today

Gasman added during his discussion, "Quantum internet presupposes you have qubits on a network, and you're moving qubits around" from one machine to another. He likened it to the early days of digital telecommunications, when "you had an analog line and could digitize things and run them through the analog lines."

Quantum PCs

Such networks of quantum computers could see more on-premises quantum computing power centralized in physical locations as the industry develops quantum computers capable of storing and processing more qubits. Many of the largest computing, internet and cloud companies already are working on such machines, the latest example of which was announced this week in Google's unveiling of plans for a "Quantum AI campus" in Santa Barbara, Calif. This includes a plan "to build 1,000,000 physical qubits that work in concert inside a room-sized error-corrected quantum computer," stated Erik lucero, lead engineer, Google

Quantum AI, in a blog post. “That’s a big leap from today’s modestly-sized systems of fewer than 100 qubits.”

Companies, let alone individuals, that don’t have the deep pockets and engineering battalions of a Google, IBM or Amazon Web Services, will be hard-pressed to develop or afford their own quantum computers anytime soon. However, the notion of a quantum PC also is becoming more realistic.

Gasman said the history of computing, in which room-sized mainframes evolved to mini-computers, which evolved to PCs, suggests what’s possible. The enabling of quantum technology in smaller form factors, via smaller, less costly, increasingly higher-performance quantum processors and other materials, could lead the way to quantum PCs.

In fact, Gasman highlighted the efforts of Chinese company SpinQ, which already boasts a $50,000 quantum computer that weighs in at 55 kilograms (about 121.5 lbs) and is available in China, Taiwan and Canada. “I wouldn’t like to carry 55 kilograms around,” Gasman said, but added later, “This is the nearest we’ve got to a quantum PC and shows that something like that could be built.”

SpinQ already has a much smaller, less pricey model in the works to be made available around the end of this year. It will cost less than $5,000 and be more portable, “and that means you could almost put it into John or Jennifer’s stocking” this holiday season, Gasman quipped. “It would have to be a big stocking.”

SpinQ’s current machines are around 2 qubits in processing power, and the company’s working on more powerful machines of three or four qubits, Gasman said. This is nowhere near the heavy-hitting plans of Google and the like, and quantum PCs in cost-efficient form factors that are capable of doing much more than current PCs are likely a very long way off.

“I don’t think clouds are going away anytime soon as the methodology of choice” for accessing quantum computing power and functionality, Gasman said.

However, noting the industry’s ability to quickly advance on technology roadmaps could have some surprises in store. “Until a year ago, it was still possible to deny the practicality of quantum computing,” he said. “Disruptive technology points the way to generally accessible technology. What seems impossible today may not seem impossible next time we have this conference.”

13 Researchers Establish the First Entanglement-Based Quantum Network

by Delft University Of Technology

https://scitechdaily.com/researchers-establish-the-first-entanglement-based-quantum-network/

A team of researchers from QuTech in the Netherlands reports realization of the first multi-node quantum network, connecting three quantum processors. In addition, they achieved a proof-of-principle demonstration of key quantum network protocols. Their findings mark an important milestone towards the future quantum internet and have now been published in Science.

The quantum internet

The power of the Internet is that it allows any two computers on Earth to be connected with each other, enabling applications undreamt of at the time of its creation decades ago. Today, researchers in many labs

around the world are working towards first versions of a quantum internet – a network that can connect any two quantum devices, such as quantum computers or sensors, over large distances. Whereas today's Internet distributes information in bits (that can be either 0 or 1), a future quantum internet will make use of quantum bits that can be 0 and 1 at the same time. "A quantum internet will open up a range of novel applications, from unhackable communication and cloud computing with complete user privacy to high-precision time-keeping," says Matteo Pompili, PhD student and a member of the research team. "And like with the Internet 40 years ago, there are probably many applications we cannot foresee right now."

Towards ubiquitous connectivity

The first steps towards a quantum internet were taken in the past decade by linking two quantum devices that shared a direct physical link. However, being able to pass on quantum information through intermediate nodes (analogous to routers in the classical internet) is essential for creating a scalable quantum network. In addition, many promising quantum internet applications rely on entangled quantum bits, to be distributed between multiple nodes. Entanglement is a phenomenon observed at the quantum scale, fundamentally connecting particles at small and even at large distances. It provides quantum computers their enormous computational power and it is the fundamental resource for sharing quantum information over the future quantum internet. By realizing their quantum network in the lab, a team of researchers at QuTech – a collaboration between Delft University of Technology and TNO – is the first to have connected two quantum processors through an intermediate node and to have established shared entanglement between multiple stand-alone quantum processors.

Operating the quantum network

The rudimentary quantum network consists of three quantum nodes, at some distance within the same building. To make these nodes operate as a true network, the researchers had to invent a novel architecture that enables scaling beyond a single link. The middle node (called Bob) has a physical connection to both outer nodes (called Alice and Charlie), allowing entanglement links with each of these nodes to be established. Bob is equipped with an additional quantum bit that can be used as memory, allowing a previously generated quantum link to be stored while a new link is being established. After establishing the quantum links Alice-Bob and Bob-Charlie, a set of quantum operations at Bob converts these links into a quantum link Alice-Charlie. Alternatively, by performing a different set of quantum operations at Bob, entanglement between all three nodes is established.

Ready for subsequent use

An important feature of the network is that it announces the successful completion of these (intrinsically probabilistic) protocols with a "flag" signal. Such heralding is crucial for scalability, as in a future quantum internet many of such protocols will need to be concatenated. "Once established, we were able to preserve the resulting entangled states, protecting them from noise," says Sophie Hermans, another member of the team. "It means that, in principle, we can use these states for quantum key distribution, a quantum computation or any other subsequent quantum protocol."

Quantum Internet Demonstrator

This first entanglement-based quantum network provides the researchers with a unique testbed for developing and testing quantum internet hardware, software and protocols. “The future quantum internet will consist of countless quantum devices and intermediate nodes,” says Ronald Hanson, who led the research team. “Colleagues at QuTech are already looking into future compatibility with existing data infrastructures.” In due time, the current proof-of-principle approach will be tested outside the lab on existing telecom fiber – on QuTech’s Quantum Internet Demonstrator, of which the first metropolitan link is scheduled to be completed in 2022.

Higher-level layers

In the lab, the researchers will focus on adding more quantum bits to their three-node network and on adding higher level software and hardware layers. Pompili: “Once all the high-level control and interface layers for running the network have been developed, anybody will be able to write and run a network application without needing to understand how lasers and cryostats work. That is the end goal.”

20 May 2021

14 The Full Story of the Stunning RSA Hack Can Finally Be Told

by andy greenberg

https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/

Amid all the sleepless hours that Todd Leetham spent hunting ghosts inside his company’s network in early 2011, the experience that sticks with him most vividly all these years later is the moment he caught up with them. Or almost did.

It was a spring evening, he says, three days – maybe four, time had become a blur – after he had first begun tracking the hackers who were rummaging through the computer systems of RSA, the corporate security giant where he worked. Leetham – a bald, bearded, and curmudgeonly analyst one coworker described to me as a “carbon-based hacker-finding machine” – had been glued to his laptop along with the rest of the company’s incident response team, assembled around the company’s glass-encased operations center in a nonstop, 24-hours-a-day hunt. And with a growing sense of dread, Leetham had finally traced the intruders’ footprints to their final targets: the secret keys known as “seeds,” a collection of numbers that represented a foundational layer of the security promises RSA made to its customers, including tens of millions of users in government and military agencies, defense contractors, banks, and countless corporations around the world.

RSA kept those seeds on a single, well-protected server, which the company called the “seed warehouse.” They served as a crucial ingredient in one of RSA’s core products: SecurID tokens – little fobs you carried in a pocket and pulled out to prove your identity by entering the six-digit codes that were constantly updated on the fob’s screen. If someone could steal the seed values stored in that warehouse, they could potentially clone those SecurID tokens and silently break the two-factor authentication they offered, allowing hackers to instantly bypass that security system anywhere in the world, accessing anything from bank accounts to national security secrets.

Now, staring at the network logs on his screen, it looked to Leetham like these keys to RSA’s global kingdom had already been stolen.

Leetham saw with dismay that the hackers had spent nine hours methodically siphoning the seeds out of the warehouse server and sending them via file-transfer protocol to a hacked server hosted by Rackspace, a cloud-hosting provider. But then he spotted something that gave him a flash of hope: The logs included the stolen username and password for that hacked server. The thieves had left their hiding place wide open, in plain sight. Leetham connected to the faraway Rackspace machine and typed in the stolen credentials. And there it was: The server's directory still contained the entire pilfered seed collection as a compressed .rar file.

Using hacked credentials to log into a server that belongs to another company and mess with the data stored there is, Leetham admits, an unorthodox move at best – and a violation of US hacking laws at worst. But looking at RSA's stolen holiest of holies on that Rackspace server, he didn't hesitate. "I was going to take the heat," he says. "Either way, I'm saving our shit." He typed in the command to delete the file and hit enter.

Moments later, his computer's command line came back with a response: "*File not found.*" He examined the Rackspace server's contents again. It was empty. Leetham's heart fell through the floor: The hackers had pulled the seed database off the server seconds before he was able to delete it.

After hunting these data thieves day and night, he had "taken a swipe at their jacket as they were running out the door," as he says today. They had slipped through his fingers, escaping into the ether with his company's most precious information. And though Leetham didn't yet know it, those secrets were now in the hands of the Chinese military.

THE RSA BREACH, when it became public days later, would redefine the cybersecurity landscape. The company's nightmare was a wake-up call not only for the information security industry – the worst-ever hack of a cybersecurity firm to date – but also a warning to the rest of the world. Timo Hirvonen, a researcher at security firm F-Secure, which published an outside analysis of the breach, saw it as a disturbing demonstration of the growing threat posed by a new class of state-sponsored hackers. "If a security company like RSA cannot protect itself," Hirvonen remembers thinking at the time, "how can the rest of the world?"

The question was quite literal. The theft of the company's seed values meant that a critical safeguard had been removed from thousands of its customers' networks. RSA's SecurID tokens were designed so that institutions from banks to the Pentagon could demand a second form of authentication from their employees and customers beyond a username and password – something physical in their pocket that they could prove they possessed, thus proving their identity. Only after typing in the code that appeared on their SecurID token (a code that typically changed every 60 seconds) could they gain access to their account.

The SecurID seeds that RSA generated and carefully distributed to its customers allowed those customers' network administrators to set up servers that could generate the same codes, then check the ones users entered into login prompts to see if they were correct. Now, after stealing those seeds, sophisticated cyberspies had the keys to generate those codes without the physical tokens, opening an avenue into any account for which someone's username or password was guessable, had already been stolen, or had been reused from another compromised account. RSA had added an extra, unique padlock to millions of doors around the internet, and these hackers now potentially knew the combination to every one.

This past December, when it became public that the company SolarWinds was hacked by Russian spies, the world woke up to the notion of a "supply chain attack": a technique in which an adversary compromises a point of vulnerability in a software or hardware supplier positioned upstream from – and out of sight of – its target, a blind spot in the victim's view of their cybersecurity risks. The Kremlin operatives who

hacked SolarWinds hid espionage code in an IT management tool called Orion, used by as many as 18,000 companies and institutions globally.

Using the SolarWinds supply chain compromise, Russia's foreign intelligence agency, known as the SVR, penetrated deep into at least nine US federal agencies, including the State Department, the US Treasury, the Department of Justice, and NASA. In another world-shaking supply chain attack just a few years earlier, Russia's military intelligence agency, known as the GRU, hijacked a piece of obscure Ukrainian accounting software to push out a data-destroying worm known as **NotPetya**, inflicting $10 billion in damage worldwide in the worst cyberattack in history.

For those with a longer memory, though, the RSA breach was the original massive supply chain attack. State cyberspies – who were later revealed to be working in the service of China's People's Liberation Army – penetrated infrastructure relied on across the globe to protect the internet. And in doing so, they pulled the rug out from under the entire world's model of digital security. "It opened my eyes to supply chain attacks," says Mikko Hypponen, chief research officer at F-Secure, who worked with Hirvonen on the company's analysis of the RSA breach. "It changed my view of the world: the fact that, if you can't break into your target, you find the technology that they use and break in there instead."

In the decade that followed, many key RSA executives involved in the company's breach have held their silence, bound by 10-year nondisclosure agreements. Now those agreements have expired, allowing them to tell me their stories in new detail. Their accounts capture the experience of being targeted by sophisticated state hackers who patiently and persistently take on their most high-value networked targets on a global scale, where an adversary sometimes understands the interdependencies of its victims' systems better than victims do themselves, and is willing to exploit those hidden relationships.

After 10 years of rampant state-sponsored hacking and supply chain hijacks, the RSA breach can now be seen as the herald of our current era of digital insecurity – and a lesson about how a determined adversary can undermine the things we trust most.

ON MARCH 8, 2011, a brisk late-winter day, Todd Leetham finished a smoke break and was walking back into RSA's headquarters in Bedford, Massachusetts – a pair of connected buildings on the edge of a forest in the Boston suburbs – when a systems administrator pulled him aside and asked him to take a look at something strange.

The admin had noticed that one user had accessed a server from a PC that the user didn't typically work on, and that the permissions setting on the account seemed unusual. A technical director investigating the anomalous login with Leetham and the admin asked Bill Duane, a veteran RSA engineer, to take a look. To Duane, who was busy working on a cryptographic algorithm at the time, the anomaly hardly looked like cause for alarm. "I frankly thought this administrator was crazy," he remembers. "Fortunately he was stubborn enough to insist that something was wrong."

Leetham and the company's security incident responders started to trace the aberrant behavior and analyze the forensics of every machine the anomalous account had touched. They began to see more telltale oddities in employees' credentials, stretching back days. The admin had been right. "Sure enough," Duane says, "this was the tip of the iceberg."

Over the next several days, the security team at RSA's security operations center – a NASA-style control room with rows of desks and monitors covering one wall – meticulously traced the interlopers' fingerprints. The RSA staffers began putting in nearly 20-hour workdays, driven by the chilling knowledge that the breach they were tracking was still unfolding. Management demanded updates on their findings every four hours, day or night.

The analysts eventually traced the origin of the breach to a single malicious file that they believed had landed on an RSA employee's PC five days before they'd started their hunt. A staffer in Australia had received an email with the subject line "2011 Recruitment plan" and an Excel spreadsheet attached to it. He'd opened it. Inside the file was a script that exploited a zero-day vulnerability – a secret, unpatched security flaw – in Adobe Flash, planting a common piece of malicious software called Poison Ivy on the victim's machine.

That initial point of entry onto RSA's network, F-Secure's Hirvonen would later point out in his own analysis, wasn't particularly sophisticated. A hacker wouldn't have even been able to exploit the Flash vulnerability if the victim had been running a more recent version of Windows or Microsoft Office, or if he'd had limited access to install programs on his PC – as most security administrators for corporate and government networks recommend, Hirvonen says.

But it was from this ingress that the RSA analysts say the intruders began to demonstrate their real abilities. In fact, several RSA executives came to believe that at least two groups of hackers were in their network simultaneously – one highly skilled group exploiting the other's access, perhaps, with or without their knowledge. "There's the trail through the woods that the first one left, and right in the middle of it, branching off, is the second trail," says Sam Curry, who was RSA's chief security officer at the time. "And that second attack was much more skilled."

On that Australian employee's PC, someone had used a tool that pulled credentials out of the machine's memory and then reused those usernames and passwords to log into other machines on the network. They'd then scraped those computers' memories for more usernames and passwords – finding some that belonged to more privileged administrators. The hackers eventually got to a server containing hundreds of users' credentials. Today that credential-stealing hopscotching technique is common. But in 2011 the analysts were surprised to see how the hackers fanned out across the network. "It was really just the most brutal way to blow through our systems that I'd ever seen," Duane says.

Breaches as extensive as the one carried out against RSA are often discovered months after the fact, when the intruders are long gone or lying dormant. But Duane says that the 2011 incident was different: Within days, the investigators had essentially caught up to the intruders and were watching them in action. "They'd try to get into a system, then we'd detect them a minute or two later and go in and shut down that system or disable access to it," Duane says. "We were fighting them tooth and nail, in real time."

It was in the midst of that feverish chase that Leetham caught the hackers stealing what he still believes was their highest-priority target: the SecurID seeds.

RSA executives told me that the part of their network responsible for manufacturing the SecurID hardware tokens was protected by an "air gap" – a total disconnection of computers from any machine that touches the internet. But in fact, Leetham says, one server on RSA's internet-connected network was linked, through a firewall that allowed no other connections, to the seed warehouse on the manufacturing side. Every 15 minutes, that server would pull off a certain number of seeds so that they could be encrypted, written to a CD, and given to SecurID customers. That link was necessary; it allowed RSA's business side to help customers set up their own server that could then check users' six-digit code when it was typed into a login prompt. Even after the CD was shipped to a client, those seeds remained on the seed warehouse server as a backup if the customer's SecurID server or its setup CD were somehow corrupted.

Now, instead of the usual once-every-15-minutes connections, Leetham saw logs of thousands of continuous requests for data every second. What's more, the hackers had been collecting those seeds on not one but three compromised servers, relaying requests through the one connected machine. They

had packaged up the collection of seeds in three parts, moved them off to the faraway Rackspace server, and then recombined them into what appeared to be the full database of every seed RSA had stored in the seed warehouse. “I was like, ‘Wow ,’” Leetham says. “I kind of admired it. But at the same time: ‘Oh crap.’”

As it dawned on Leetham that the seed collection had likely been copied – and after he had made his seconds-too-late attempt to delete the data off the hackers’ server – the enormity of the event hit him: The trust that customers placed in RSA, perhaps its most valuable commodity, was about to be obliterated. “This is an extinction event,” he remembers thinking. “RSA is over.”

IT WAS LATE at night when the security team learned that the seed warehouse had been plundered. Bill Duane made the call: They would physically cut off as many of RSA’s network connections as necessary to limit the damage and stop any further theft of data. They hoped, in particular, to protect any customer information that mapped to the seeds, and which might be necessary for the hackers to exploit them. (Some RSA staff also suggested to me that the seeds had been stored in an encrypted state, and cutting off network connections was intended to prevent the hackers from stealing the key necessary to decrypt them.) Duane and an IT manager walked into the data center and started unplugging Ethernet cables one by one, severing the company’s connections to its manufacturing facility, parts of its network that handled core business processes like customer orders, even its website. “I basically shut off RSA’s business,” he says. “I crippled the company in order to stop any potential further release of data.”

The next day, RSA’s CEO, Art Coviello, was in a meeting in the conference room that adjoined his office, preparing a public statement about the ongoing breach. Coviello had been getting updates since the intrusions were discovered. As the extent of the breach had grown, he’d canceled a business trip to Brazil. But he’d remained relatively sanguine. After all, it didn’t sound like the hackers had breached any credit card data or other sensitive customer information. They’d kick out the hackers, he figured, post their statement, and get on with business.

But in the middle of the meeting, he remembers, a marketing executive at the table with him looked at her phone and murmured, “Oh dear.”

Coviello asked her what was wrong. She demurred. He took the phone out of her hand and read the message. It said that Bill Duane was coming up to Coviello’s office; he wanted to update the CEO in person. When he got upstairs, he delivered the news: The hackers had reached the SecurID seeds. “I felt like a cannonball had been shot through my stomach,” Coviello says.

In the hours that followed, RSA’s executives debated how to go public. One person in legal suggested they didn’t actually need to tell their customers, Sam Curry remembers. Coviello slammed a fist on the table: They would not only admit to the breach, he insisted, but get on the phone with every single customer to discuss how those companies could protect themselves. Joe Tucci, the CEO of parent company EMC, quickly suggested they bite the bullet and replace all 40 million-plus SecurID tokens. But RSA didn’t have nearly that many tokens available – in fact, the breach would force it to shut down manufacturing. For weeks after the hack, the company would only be able to restart production in a diminished capacity.

As the recovery effort got under way, one executive suggested they call it Project Phoenix. Coviello immediately nixed the name. “Bullshit,” he remembers saying. “We’re not rising from the ashes. We’re going to call this project Apollo 13. We’re going to land the ship without injury.”

AT 7:00 THE next morning, March 17, RSA’s head of North American sales, David Castignola, finished up an early workout on a treadmill at his local gym in Detroit. When he picked up his phone, he saw that he had missed no fewer than 12 calls – all from just that morning, and all from RSA’s president, Tom

Haiser. RSA, Haiser's voicemails said, was about to announce a major security breach. He needed to be in the building.

A few hours and a last-minute flight later, Castignola literally ran into RSA's headquarters in Bedford and up to the fourth-floor conference room. He immediately noticed the pale, drawn faces of the staff who had been dealing with the unfolding crisis for more than a week. "Every little indicator I got was: This is worse than I can even get my head around," Castignola remembers.

That afternoon, Coviello published an open letter to RSA's customers on the company's website. "Recently, our security systems identified an extremely sophisticated cyberattack in progress," the letter read. "While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack," the letter continued – somewhat downplaying the crisis.

In Bedford, Castignola was given a conference room and the authority to ask for as many volunteers from the company as he needed. A rotating group of nearly 90 staffers began the weeks-long, day-and-night process of arranging one-on-one phone calls with every customer. They worked from a script, walking customers through protective measures like adding or lengthening a PIN number as part of their SecurID logins, to make them harder for hackers to replicate. Castignola remembers walking down the halls of the building at 10 pm and hearing calls on speaker phones behind every closed door. In many cases customers were shouting. Castignola, Curry, and Coviello each did hundreds of those calls; Curry began to joke that his title was "chief apology officer."

At the same time, paranoia was beginning to take hold in the company. The first night after the announcement, Castignola remembers walking by a wiring closet and seeing an absurd number of people walking out of it, far more than he imagined could have ever fit. "Who are those people?" he asked another nearby executive. "That's the government," the executive responded vaguely.

In fact, by the time Castignola had landed in Massachusetts, both the NSA and the FBI had been called to help the company's investigation, as had defense contractor Northrop Grumman and incident response firm Mandiant. (By chance, employees of Mandiant had already been on-site prior to the breach, installing security sensor equipment on RSA's network.)

RSA staff began to take drastic measures. Worried that their phone system might be compromised, the company switched carriers, moving from AT&T to Verizon phones. Executives, not trusting even the new phones, held meetings in person and shared paper copies of documents. The FBI, fearing an accomplice in RSA's ranks because of the apparent level of knowledge the intruders seemed to have of company systems, started doing background checks. "I made sure that all members of the team – I don't care who they were, what reputation they had – were investigated, because you have to be sure," Duane says.

The windows of some executives' offices and conference rooms were covered in layers of butcher paper, to prevent laser microphone surveillance – a long-distance eavesdropping technique that picks up conversations from vibrations in window panes – by imagined spies in the surrounding woods. The building was swept for bugs. Multiple executives insisted that they did find hidden listening devices – though some were so old that their batteries were dead. It was never clear if those bugs had any relation to the breach.

Meanwhile, RSA's security team and the investigators brought in to help were "tearing the house down to the studs," as Curry put it. In every part of the network that the hackers touched, he says, they scrubbed the contents of potentially compromised machines – and even ones adjacent to them. "We physically went around and, if there was a box they were on, it got wiped," Curry says. "If you lost data, too bad."

IN LATE MAY 2011, about two months after the breach announcement, RSA was still recovering, rebuilding, and apologizing to customers when it was hit with an aftershock: A post appeared on the influential tech blogger Robert X. Cringely's website, titled "*InsecureID: No More Secrets?*"

The post was based on a tip from a source inside a major defense contractor, who'd told Cringely that the company was responding to an extensive intrusion by hackers who seemed to have used stolen RSA seed values to get in. Everyone at the defense contractor was having their RSA tokens replaced. Suddenly RSA's breach seemed far more severe than the company's original announcement had described it. "Well it didn't take long for whoever cracked RSA to find a lock to fit that key," Cringely wrote. "What if every RSA token has been compromised, everywhere?"

Two days later, Reuters revealed the name of the hacked military contractor: Lockheed Martin, a company that represented a cornucopia of ultra-secret plans for weapons and intelligence technologies. "The scab was healing," Castignola says. "Then Lockheed hit. That was like a mushroom cloud. We were back at it again."

In the days that followed, defense contractors Northrop Grumman and L-3 were also named in news reports. Hackers with SecurID's seed values had targeted them too, the stories said, though it was never clear how deeply the intruders had penetrated the companies. Nor was it revealed what the hackers had accessed inside Lockheed Martin. The company claimed it had prevented the spies from stealing sensitive information like customer data or classified secrets.

In another open letter to customers in early June 2011, RSA's Art Coviello admitted, "We were able to confirm that information taken from RSA in March had been used as an element of an attempted broader attack on Lockheed Martin, a major US government defense contractor."

Today, with 10 years of hindsight, Coviello and other former RSA executives tell a story that starkly contradicts accounts from the time: Most of the former RSA staff who spoke to me claim that it was never proven that SecurID had any role in the Lockheed breach. Coviello, Curry, Castignola, and Duane all argued that it was never confirmed that the intruders inside RSA's systems had successfully stolen the full list of seed values in an uncorrupted, unencrypted form, nor the customer list mapped to those seeds necessary to exploit them. "I don't think that Lockheed's attack was related to us at all," Coviello states flatly.

By contrast, in the years since 2011, Lockheed Martin has detailed how hackers used information stolen in RSA's SecurID breach as a stepping stone to penetrate its network – even as it insists that no information was successfully stolen in that event. A Lockheed source with knowledge of the company's incident response reaffirmed to WIRED the company's original claims. "We stand by our forensic investigation findings," the source says. "Our analysis determined the breach of our two-factor authentication token provider was a direct contributing factor in the attack on our network, a fact that has been widely reported by the media and acknowledged publicly by our vendor, including Art." In fact, the Lockheed source says the company saw the hackers entering SecurID codes in real time, confirmed that the targeted users hadn't lost their tokens, and then, after replacing those users' tokens, watched the hackers continue to unsuccessfully enter codes from the old tokens.

The NSA, for its part, has never had much doubt about RSA's role in subsequent break-ins. In a briefing to the Senate Armed Services Committee a year after the RSA breach, NSA's director, General Keith Alexander, said that the RSA hack "led to at least one US defense contractor being victimized by actors wielding counterfeit credentials," and that the Department of Defense had been forced to replace every RSA token it used.

In the hearing, Alexander went on to pin those attacks, vaguely, on an increasingly common culprit: China. The New York Times and the security firm Mandiant would later publish a groundbreaking exposé on a Chinese state hacker group that Mandiant had named APT1. The group was believed to be People's Liberation Army Unit 61398, based on the outskirts of Shanghai. Among its dozens of targets over the previous five years: the governments of the United States, Canada, South Korea, Taiwan, Vietnam; and the United Nations – and RSA.

After those reports became public, Bill Duane printed out a picture of the hackers' headquarters, a 12-story white building off of Shanghai's Datong Road. He taped it to a dartboard in his office.

I ASKED DUANE, who retired from RSA in 2015 after more than 20 years at the company, at what point he considered RSA's breach truly over: Was it the morning after he made the lonely decision to unplug a chunk of the company's network? Or when the NSA, the FBI, Mandiant, and Northrop had wrapped up and left? "Our view was that the attack wasn't ever over," he responds. "We knew that they left backdoors, that they're always going to be able to break in, that the attacker can, with their resources, get in when they want to get in."

Duane's harrowing experience in response to the intrusion taught him – and perhaps should teach all of us – that "every network is dirty," as he puts it. Now he preaches to companies that they should segment their systems and cordon off their most sensitive data so that it remains impenetrable even to an adversary that's already inside the firewall.

As for Todd Leetham, he watched the SolarWinds fiasco unfold over the past six months with a grim sense of déjà vu. "Everybody was shocked. But in hindsight, well, duh, it was kind of everywhere," he says of SolarWinds. As was, by analogy, SecurID, 10 years earlier.

Leetham sees the lessons of RSA's supply chain compromise in starker terms than even his colleague Bill Duane: It was "a glimpse of just how fragile the world is," he says. "It's a house of cards during a tornado warning."

SolarWinds demonstrated how precarious this structure remains, he argues. As Leetham sees it, the security world blindly put its trust in something that existed outside its threat model, never imagining that an adversary might attack it. And once again, the adversary pulled out a supporting card underpinning the house's foundation – one that had been confused for solid ground.

18 May 2021

15 quantum computing: the chronicle of its origin and beyond

by Meenu EG

https://www.analyticsinsight.net/quantum-computing-the-chronicle-of-its-origin-and-beyond/

The spark about quantum computing is considered to have set out from a three-day discussion at the MIT Conference Center out of Boston, in 1981. The meeting, '*The Physics of Computation*', was collaboratively sponsored by IBM and MIT's Laboratory of computer science. The discussion aimed to formulate new processes for efficient ways of computing and bring the area of study into the mainstream. Quantum computing was not a popularly discussed field of science till then. The historic conference was presided over by many talented brains including **Richard Feynman, Paul Benioff, Edward Fredkin, Leonid Levin, Freeman Dyson,** and **Arthur Burks**, who were computer scientists and physicists.

Richard Feynman was a renowned theoretical physicist who received a Nobel Prize in Physics, in 1965 with other two physicists, for his contributions towards the development of quantum electrodynamics. The conference was a seminal moment in the development of quantum computing and Richard Feynman announced that to simulate quantum computation, there is a need for quantum computers. Later, he went on to publish a paper in 1982, titled 'Simulating Physics with Computers'. The area of study soon got attention from computer scientists and physicists. Hence, the work on quantum computing began.

Before this, in 1980, Paul Benioff had described a first quantum mechanical model of a computer in one of his papers, which had already acted as a foundation for the study. After Feynman's statement in the conference, Paul Benioff went on to develop his model of quantum mechanical Turing machine.

However, almost a decade later, came Shor's algorithm, developed by Peter Shor, which is considered a milestone in the history of quantum computing. This algorithm allowed quantum computers to factor large integers at a higher speed and could also break numerous cryptosystems. The discovery garnered a lot of interest in the study of quantum computing as it replaced the years taken by the classic, traditional computing algorithms to perform factoring by just some hours. Later, in 1996, Lov Grover invented the quantum database search algorithm, which exhibited a quadratic speedup that could solve any problem that had to be solved by random brute-force search and could also be applied to a wider base of problems.

The year 1998 witnessed the first experimental demonstration of a quantum algorithm that worked on a 2-qubit NMR quantum computer. Later in the year, a working 3-qubit NMR computer was developed and Grover's algorithm got executed for the first time in an NMR quantum computer. Several experimental progress took place between 1999 and 2009.

In 2009, the first universal programmable quantum computer was unveiled by a team at the National Institute of Standards and Technology, Colorado. The computer was capable of processing 2 quantum bits.

After almost a decade, IBM unveiled the first commercially usable integrated quantum computing system, and later in the year, IBM added 4 more quantum computing systems, along with a newly developed 53-qubit quantum computer. Google also gave a huge contribution to the field in late 2019, when a paper published by the Google research team claimed to have reached quantum supremacy. The 54-qubit Sycamore processor, made of tiny qubits and superconducting materials is claimed to have sampled a computation in just 200 seconds. Last year, IonQ launched its trapped ion quantum computers and made them commercially available through the cloud. There have been several experiments and research that are being carried on today. Each day becomes a new step for quantum computing technology since its proclamation back in the 80s.

According to a report by Fast Company, IBM plans to complete the 127-qubit IBM Quantum Eagle this year and expects to develop a 1000-qubit computing machine called the **IBM Quantum Condor** by 2023. IBM has been keeping up in the path of developing the best quantum computing solutions since it hosted the conference in 1981. Charlie Bennet, a renowned physicist who was part of the conference as IBM's research contingent, has a huge contribution to these innovations put forward by the company.

The emerging era of quantum computing will invite many breakthroughs. The quantum computing revolution will increase processing efficiency and solve intrinsic quantum problems. Quantum computer works with quantum bits or qubits that can be in the 'superposition of states that will cater to massive calculations at an extremely faster pace.

Quantum computing will have a greater impact on almost all industries and business operations. It is capable of molecular modeling, cryptography, weather forecasting, drug discovery, and more. Quantum computing is also said to be a significant component of artificial intelligence, which is fuelling several

businesses and real-life functions today. We might soon reach the state of quantum supremacy and businesses need to become quantum-ready by then.

16 Google Aims for Commercial-Grade Quantum Computer by 2029

by Sara Castellanos

https://www.wsj.com/amp/articles/google-aims-for-commercial-grade-quantum-computer-by-2029-11621359156#amp_tf=From%20%251%24s&aoh=16213785676148&csi=1&referrer=https%3A%2F%2Fwww.google.com

Alphabet Inc.'s Google plans to spend several billion dollars to build a quantum computer by 2029 that can perform large-scale business and scientific calculations without errors, said Hartmut Neven, a distinguished scientist at Google who oversees the company's Quantum AI program. The company recently opened an expanded California-based campus focused on the effort, he said.

"We are at this inflection point," said Dr. Neven, who has been researching quantum computing at Google since 2006. "We now have the important components in hand that make us confident. We know how to execute the road map."

Chief Executive Sundar Pichai announced the timeline and introduced the new Google Quantum AI campus in Santa Barbara County on Tuesday at Google's annual developer conference.

"Quantum computing represents a fundamental shift, because it harnesses the properties of quantum mechanics and gives us the best chance of understanding the natural world," Mr. Pichai said at the virtual event.

Google, which has been investing in the nascent technology for several years, is one of many companies including International Business Machines Corp. , D-Wave Systems Inc. and Honeywell International Inc. working to commercialize it. IBM and others have recently announced technological developments and planned milestones related to quantum computing within the next few years. Dario Gil, director of IBM Research, recently said 2023 would be an inflection point in that the errors of quantum computers would continue to decrease exponentially through software, as opposed to just hardware.

A commercial-grade quantum computer doesn't yet exist, but eventually it could solve some problems many millions of times faster than a conventional computer. Companies such as Visa Inc., JPMorgan Chase & Co. and Volkswagen AG are experimenting with early-stage quantum technology.

By harnessing quantum physics, this type of computing has the potential to sort through vast numbers of possibilities in nearly real time and come up with a probable solution. Traditional computers store information as either zeros or ones. Quantum computers use quantum bits, or qubits, which represent and store information in a quantum state that is a complex mix of zero and one.

Google, like many other companies investing in quantum computing, plans to offer its commercial-grade quantum-computing services over the cloud. Google is interested in many potential uses for the technology, such as building more energy-efficient batteries, creating a new process of making fertilizer that emits less carbon dioxide and speeding up training for machine-learning, a branch of artificial intelligence, Dr. Neven said.

For those and other use cases, Google says it will need to build a 1-million-qubit machine capable of performing reliable calculations without errors. Its current systems have less than 100 qubits.

There are numerous challenges to contend with, Dr. Neven said. For example, Google will need to work

on lengthening the time that the qubits remain in their quantum state, because they are susceptible to disturbances in temperature, frequency and motion. Such changes can hurt the accuracy of a calculation or prevent it from being completed.

Google's new Quantum AI campus is an expansion of its experimental lab space. Many of its researchers have ties to the University of California, Santa Barbara. The campus includes a quantum-data center, research labs and chip-fabrication facilities spanning several buildings, one of which features colorful stained-glass artwork made by a California-based artist.

Construction on the expansion began in 2019, was delayed for a few months by pandemic-related work restrictions, and was officially completed in late 2020, said Erik Lucero, a quantum-computing research scientist at Google who led the design and construction of the campus. Hundreds of employees are expected to work there over the next few years, he said.

The pace of innovation in quantum computing over the last five years exceeds that of the past three decades, said Chirag Dekate, vice president analyst at technology research firm Gartner Inc. The field, however, is extremely complex and there are challenges in translating traditional algorithms into quantum-based algorithms, he said. "These initiatives are inherently challenging and risk for road-map slippage across vendors is high," he said.

By 2025, nearly 40% of large companies are expected to create quantum-computing initiatives, according to Gartner. The global market for quantum-computing hardware will exceed $7.1 billion by 2026, according to Research and Markets, another research firm.

Public cloud providers such as Amazon.com Inc., Microsoft Corp. and Google are investing heavily in next-generation computing techniques, including quantum, as it becomes increasingly difficult to eke out performance gains in traditional chips, Mr. Dekate said.

Inquiries from tech executives at enterprise companies on the topic of quantum computing have increased by 28% since last year, Mr. Dekate said.

Google has lagged behind others such as IBM and D-Wave in commercializing access to experimental quantum-computing machines, Mr. Dekate said. "That's going to be the biggest test for Google, is how they engage enterprise audiences," he added.

Google has been offering companies and academics the chance to experiment with its early-stage quantum-computing technology since last year, Dr. Neven said. More enterprises and researchers will be able to access the services in the coming years, he said.

17 May 2021

17 How Quantum Xchange solves for the PQC Adoption Challenges Outlined by NIST

https://quantumxc.com/how-quantum-xchange-solves-for-the-pqc-adoption-challenges-outlined-by-nist/?utm_medium=email&utm_source=newsletter&utm_campaign=may21

Most professionals in the security industry understand the pains, challenges, and time it takes to complete a cryptographic transition. It took more than 20 years for the Advanced Encryption Standard (AES) to completely replace Data Encryption Standard (DES) and 3DES. If you haven't heard the noise, a quantum computer will be able to break RSA-2048, considered the gold standard for Public Key Encryption (PKE),

the system that has for years protected our digital universe.

In 2016 the National Institute for Standards and Technology (NIST) warned that all organizations start preparing then for the coming quantum-crypto break. Unfortunately, most have made very little, if any, movement to heed this advice. Our partners at Thales released an industry survey that found 72% of organizations see quantum computing affecting them in the next five years. However, in a similar survey conducted by DigiCert only 56% of organizations surveyed were learning quantum-safe practices.

Unlike Y2K, when there was a definitive deadline and end-date to work against, Y2Q is ambiguous causing too many companies to take a lackadaisical, wait and see attitude to quantum preparedness planning and execution. Many are waiting for the Post-Quantum Cryptography (PQC) selection process by NIST to yield the final standard before they take action.

This is flawed, shortsighted thinking. Consider the following:

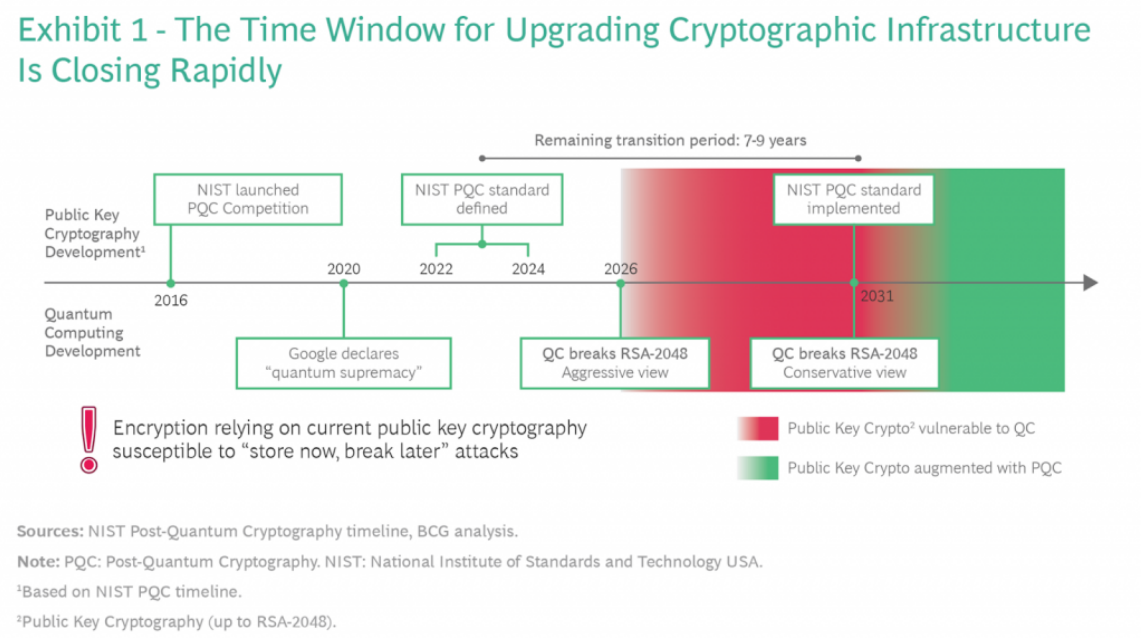
- A quantum computer may be available before the final PQC selection process is finalized and the full transition is completed. Google CEO Sundar Pichai at Davos 2020 said he expects that quantum computing will break encryption as we know it in the next 5-10 years.
- There is no guarantee that the cryptographic standards selected will not be broken by adversaries or vulnerable to implementation errors. Some even argue a quantum attack by a nation-state could occur without anyone's knowledge. Roger Grimes, author of the book **Cryptography Apocalypse** goes a step further to announce, "I predict that someone will publicly announce that they have used a quantum computer to break a traditional asymmetric key cipher. It's been the Holy Grail since 1994 and I predict it happens next year."
- Harvest today, decrypt tomorrow attacks are happening now.
- Current PKE systems, i.e., TLS/SSL and key management practices are rife with vulnerabilities putting today's data and communications networks at risk. With PKE, the encryption keys and data travel together. An attacker needs only to compromise one connection to obtain secret information.

Last week, NIST published the final version of its report titled, Getting Ready for Post-Quantum Cryptography outlining the challenges associated with adopting and using PQC algorithms after the standardization process is complete – which is currently on pace for selection by 2022-24. NIST also cautions that in the best case, another 5-15 more years will be needed after the publication of the cryptographic standards before a full transition is completed.

Boston Consulting Group (BCG), in its March 30, 2021 article, "Ensuring Online Security in a Quantum Future" (see our take on this informative, must-read article here) published the below timeline in response to the NIST PQC project and warned, "This implies that window for upgrading existing infrastructure is seven to nine years – too short for such an ambitious goal." In concluding, "companies in all industries need to take note now and plan for encryption in the quantum future now."

Quantum Xchange understands the challenges and complexities of cryptographic transitions can be overwhelming, if not paralyzing. We've built a practical and highly scalable, quantum-safe key distribution system that allows organizations to get started now with very little lift or outlay. In fact, our affordable, crypto-agile path to quantum safety can be easily dropped into organizations' existing crypto infrastructure today.

Phio Trusted Xchange (TX) is a simple architecture overlay that leverages a patent-pending out-of-band symmetric key delivery technology to supplement native encryption with an additional key-encrypting-key



(KEK) transmitted independently of the data path. The system supports quantum keys from any source i.e., PQC (all candidate KEM algorithms), QKD, QRNG, or combination. Organizations can easily increase quantum protection levels based on their data inventory requirements and risk tolerance levels without any disruption to the network.

18 4th generation of Quantum Key Distribution XG Series

by ID Quantique

https://www.idquantique.com/id-quantique-unveils-its-4th-generation-of-quantum-key-distribution-qkd-the-cerberis-xg-the-ultimate-in-quantum-safe-security/

Safety of current encryption methods, and especially of the key exchange mechanisms based on asymmetric cryptography, is a major concern today particularly for governments and enterprises which must protect data for five to ten years or more. Possible back-doors in current systems combined with massive computing power already put high-value sensitive data at risk of being decrypted by malevolent actors. Moreover, the arrival of quantum computers is imminent and will render asymmetric key exchanges unsafe: encrypted data can be stored now and easily decrypted later.

As a leading security solution provider and since 2007, IDQ has commercialized Quantum Key Distribution (QKD) that generates and distributes cryptographic keys across a provably secure communication network, to safely encrypt or authenticate data. Its products are used by governments, enterprises, industrial customers, and by academic research labs in more than 60 countries and on every continent.

Today, based on 14 years of commercial deployment and customer feedbacks, IDQ is launching its 4th generation of Cerberis series.

IDQ's Cerberis XG is smaller (1U compact chassis), provides higher value, is easy to operate and it can easily interface with link encryptors from major vendors on the market.

It also embeds enhanced trusted security components, such as tamper detection, a secure memory module as well as IDQ's latest QRNG technology (IDQ20MC1 QRNG chip) which provides proven randomness for all the related crypto storage. In contrast to conventional key distribution algorithms, QKD is the only known cryptographic technique which offers forward security, resilient to new attack algorithms and upcoming quantum computers. A significant advantage of QKD technology resides in the fact that its reliability is not impacted by technological advancements nor time.

ID Quantique's leadership team will present the new Cerberis XG during virtual event Inside Quantum Technology (IQT), the premier conference dedicated to the business of quantum computing, quantum networking, quantum sensors, and quantum technology. The conference gets underway today with "Year 2 in the Quantum Decade – Time to Act" – an opening keynote session by Axel Foery, Executive VP Quantum-Safe Security at ID Quantique., who will address quantum security focusing on Quantum Random Number Generators (QRNG) and Quantum Key Distribution (QKD) with a technology outlook on the next couple of quarters. IDQ's team will also share experience from twenty years of innovation, participating in a number of panels throughout the 4-day conference.

19 Three Common Misconceptions About Quantum Technology

https://quantumcomputingreport.com/three-common-misconceptions-about-quantum-technology/

We've seen an increasing number of misconceptions being spread about what quantum technology will be able to do. Admittedly, it is a complicated technology but we are concerned that overblown expectations can lead to a Quantum Winter or unwarranted investments being made in quantum technology due to misunderstandings. So in this article we are highlighting some of the more obvious misconceptions about quantum technology that we have heard recently among the general public. We have actually seen three cases in the past week where one or more of these misconceptions was mentioned or implied!

- **Misconception 1: Entanglement Will Enable Information Transfer Faster than the Speed of Light**

  When people first hear about the entanglement phenomena, they come to the conclusion that this will allow information transfer faster than the speed of light. If this were true, it would have an enormous impact on things like financial markets since it would enable arbitrage that would allow traders to take advantage of slight differences in stock prices in different location. While entanglement does allow two physically separated parties to simultaneously measure random bit streams and get the same result even if they are light years apart, RANDOM BIT STREAMS $\neq$ INFORMATION. The QKD schemes that have developed can leverage this entanglement phenomena but they also require sending classical data between the two communication parties in order to complete the information transfer. Although many people have tried to develop a scheme to circumvent this fact, certain fundamental laws of quantum physics, like the No-Cloning Theorem prevent this from happening.

- **Misconception 2: If We Just Implemented Quantum Resistant Encryption Technologies, like PQC or QKD, All of Our Cybersecurity Issues Would Go Away**

  Although the threat of a quantum computer being able to break the encryption algorithms we are using today to secure the internet is real, there are many, many more ways that computer systems are vulnerable to hackers that are still possible even when quantum resistant encryption technologies

are employed. Like many things, most of the vulnerabilities can be due to human issues rather than technological issues. These could include phishing attacks, rogue employees, physical system security, and software bugs. These issues will cause the vast majority of cybersecurity problems for now and in the future. Unfortunately, this fact doesn't get in the way of market forecasts presented by companies working on quantum communication. We recently saw a slide deck that showed a Gartner forecast estimating the cybersecurity market to be about $194 billion by 2024. But what is not said in the slide is that the quantum resistant encryption portion of this amount (the PQC and QKD portions) will be less than 5% of this total spend. Unfortunately, cybersecurity is a multi-headed beast and you must combat all the different threats in order to be fully secure.

- **Misconception 3: Although It May Take 50 Years or More, Eventually Quantum Will Completely Replace All Classical Computation and Communication Approaches**

  In the 1920's, some people predicted that the future of transportation would be flying cars. The argument was that this would solve the problem of congested city streets that they were starting to experience. Of course, this never happened. While there is still talk of flying cars, no one is predicting today that the bulk of local transportation will be accomplished with flying cars. The reasons have to do with cost, conflicting requirements and safety. On the other hand, people in the 1950's were predicting that vacuum tubes based computers would be replaced by ones that were based upon transistor technology. This forecast did indeed come to pass for reasons based upon size, power, performance and most important of all, cost. Our belief is that quantum versus classical will turn out to be more similar to the flying car situation for several reasons. First, there are a great many commonly used algorithms algorithms that cannot be sped up with a quantum approach. Quantum applications are only viable if a specific algorithm is found that can compute something with exponentially fewer operations than classical. And most computational tasks are not like that. In addition, quantum devices are much more costly to produce than classical computers and no one has ever shown a roadmap these devices can ever be manufactured cheaper than a classical microprocessor. So the future computing environment will always contain a combination of classical and quantum devices much like airplanes and automobiles are used in combination today. Similar arguments can be made for networking technologies because even though quantum networking may have some advantages with regards to functionality, the classical approach will always have the edge i n both raw performance and cost. So the future will be classical and quantum working together and not quantum completely replacing classical.

14 May 2021

20 Quantum Leap for Quantum Computing: Ion Beams Create Chains of Closely Coupled Qubits

by Lawrence Berkeley National Laboratory

https://scitechdaily.com/quantum-leap-for-quantum-computing-ion-beams-create-chains-of-closely-coupled-qubits/

Achieving the immense promise of quantum computing requires new developments at every level, including the computing hardware itself. A Lawrence Berkeley National Laboratory (Berkeley Lab)-led international team of researchers has discovered a way to use ion beams to create long strings of "color center" qubits in diamond. Their work is detailed in the journal Applied Physics Letters.

The authors includes several from Berkeley Lab: Arun Persaud, who led the study, and Thomas Schenkel, head of the Accelerator Technology and Applied Physics (ATAP) Division's Fusion Science & Ion Beam Technology Program, as well as Casey Christian (now with Berkeley Lab's Physics Division), Edward Barnard of Berkeley Lab's Molecular Foundry, and ATAP affiliate Russell E. Lake.

Creating large numbers of high-quality quantum bits (qubits), in close enough proximity for coupling to each other, is one of the great challenges of quantum computing. Collaborating with colleagues worldwide, the team has been exploring the use of ion beams to create artificial color centers in diamond for use as qubits.

Color centers are microscopic defects – departures from the rigorous lattice structure of a crystal, such as diamond. The type of defect that is of specific interest for qubits is a nitrogen atom next to a vacancy, or empty space, in a diamond lattice. (Nitrogen is commonly found in the crystal lattice of diamond, which is primarily a crystalline form of carbon, and can contribute to the color of the stone.)

When excited by the rapid energy deposition of a passing ion, nitrogen-vacancy centers can form in the diamond lattice. The electron and nuclear spins of nitrogen-vacancy centers and the adjacent carbon atoms can all function as solid-state qubits, and the crystal lattice can help protect their coherence and mutual entanglement.

The result is a physically durable system that does not have to be used in a cryogenic environment, which are attractive attributes for quantum sensors and also for qubits in this type of solid-state quantum computer. However, making enough qubits, and making them close enough to each other, has been a challenge.

When swift (high-energy) heavy ions such as the beams this team used – gold ions with a kinetic energy of about one billion electron volts – pass through a material, such as nitrogen-doped diamond, they leave a trail of nitrogen-vacancy centers along their tracks. Color centers were found to form directly, without need for further annealing (heat treatment). What's more, they formed all along the ion tracks, rather than only at the end of the ion range as had been expected from earlier studies with lower-energy ions. In these straight "percolation chains," color-center qubits are aligned over distances of tens of microns, and are just a few nanometers from their nearest neighbors. A technique developed by Berkeley Lab's Molecular Foundry measured color centers with depth resolution.

The work on qubit synthesis far from equilibrium was supported by the Department of Energy's Office of Science. The next step in the research will be to physically cut out a group of these color centers – which are like a series of beads on a string – and show that they are indeed so closely coupled that they can be used as quantum registers.

Results published in the current article show that it will be possible to form quantum registers with up to about 10,000 coupled qubits – two orders of magnitude greater than achieved thus far with the complementary technology of ion-trap qubits – over a distance of about 50 microns (about the width of a human hair).

"Interactions of swift heavy ions with materials have been studied for decades for a variety of purposes, including the behavior of nuclear materials and the effects of cosmic rays on electronics," said Schenkel.

He added that researchers worldwide have sought to make quantum materials by artificially inducing color centers in diamond. "The solid-state approaches to quantum computing hardware scale beautifully, but integration has been a challenge. This is the first time that direct formation of color-center qubits along strings has been observed."

The stars, like diamonds

On a miniscule and ephemeral scale (nanometers and picoseconds) the deposition of energy by the ion beams produces a state of high temperature, which Schenkel likens to the surface of the sun, in the 5000 K range, and pressure. Besides knocking carbon atoms out of the crystal lattice of diamond, this effect could enable fundamental studies of exotic states of transient warm dense matter, a state of matter that is present in many stars and large planets and which is difficult to study directly on Earth.

It might also enable formation of novel qubits with tailored properties that cannot be formed with conventional methods. "This opens a new direction for expanding our ability to form quantum registers," said Schenkel.

Currently, color-center strings are formed with beams from large particle accelerators, such as the one at the German laboratory GSI that was used in this research. In the future, they might be made using compact laser-plasma accelerators like the ones being developed at the Berkeley Lab Laser Accelerator (BELLA) Center.

The BELLA Center is actively developing its ion-acceleration capabilities with funding by the DOE Office of Science. These capabilities will be used as part of LaserNetUS. Ion pulses from laser-plasma acceleration are very intense and greatly expand our ability to form transient states of highly excited and hot materials for qubit synthesis under novel conditions.

More facets in materials science far from equilibrium

The process of creating these color centers is interesting in its own right and has to be better understood as part of further progress in these applications. The details of how an intense ion beam deposits energy as it traverses the diamond samples, and the exact mechanism by which this leads to color-center formation, hold exciting prospects for further research.

"This work demonstrates both the discovery science opportunities and the potential for societally transformative innovations enabled by the beams from accelerators," says ATAP Division Director Cameron Geddes. "With accelerators, we create unique states of matter and new capabilities that are not possible by other means."

21 Fully integrated 'hot qubit' quantum processor using commercially available technology

by University College Dublin

https://phys.org/news/2021-05-fully-hot-qubit-quantum-processor.html

Equal1 Laboratories (Equal1), a silicon-based quantum computing company, today announced the company is the first to demonstrate a fully integrated quantum processor unit (QPU) operating at 3.7 kelvin – a major milestone with implications for the trajectory of quantum computing.

The company is addressing a major challenge for the quantum computing industry of scaling the number of qubits so that a quantum computer can tackle useful, real-world problems.

With its QPU, Equal1 has developed a disruptive, scalable and cost-effective quantum computing technology, based on a commercially available silicon semiconductor process.

The QPU employs patented, Equal1-designed, nanometer-scale quantum dots to create qubits (the quantum equivalent to digital bits) on a standard silicon CMOS process. In addition to the silicon qubits, all control and read-out electronics required for a fully functioning QPU are integrated on-chip with over 10 million transistors.

In addition to developing its QPU, Equal1 has designed and manufactured the closed cryogenic and vacuum system, together with the control and communication electronics to maintain the chip at 3.7 K and interface to room temperature.

Due to the operation of the qubits at 3.7 K (referred to as "hot qubits") and the level of integration the team has achieved, the form factor of the quantum demonstrator is far smaller than alternative technologies (rack-sized versus room-sized).

Equal1 was founded by Dirk Leipold, Mike Asker and Professor R. Bogdan Staszewski and is a spin-out from the UCD School of Electrical and Electronic Engineering. The Equal1 team has offices at NovaUCD, the Center for New Ventures and Entrepreneurs at University College Dublin, and in California.

Elena Blokhina, Equal1 CTO, said, "Our team's ability to demonstrate quantum behavior on a fully integrated QPU will enable us to soon solve challenges in AI that cannot be solved today. We are proud of the milestone accomplishment and are excited to scale our technology to the next level."

Two Equal1 quantum demonstrator machines ("Alice") each have been running for over 24 cumulative months with no unplanned downtime. On Alice, Rabi oscillations have been observed in three-dot arrays with a coherence time of 150 ns.

Due to the integrated nature of the technology, the electronic pulses that control the qubits are generated on-chip and therefore are extremely fast, enabling a short enough pulse time for the QPU to demonstrate quantum behavior. The team has proven the repeatability of the results and consistency with quantum modeling and simulations.

"By taking advantage of shrinking transistor geometries, we have demonstrated that integration into the millions of qubit range is possible, with moderate cooling requirements compared to other qubit technologies," said, Equal1 CEO, Dirk Leipold.

"Our quantum computing technology delivers affordable AI solutions to our customers at a much lower carbon footprint."

The QPU was manufactured on GlobalFoundries leading low power 22FDX platform, requiring no special process extensions for quantum operation. Employing this ultra-low power platform at GlobalFoundries Fab 1 in Dresden, Germany played a key role in enabling Equal1 to achieve the results presented here.

The Equal1 team designed the complex mixed signal circuits, such as high-speed pulse generator, ADCs, DACs and cryogenic memory, using EDA software from Cadence Design Systems, Inc., in particular Specter Simulation Platform's new support for ultra-low temperature models which are key to cryoelectronic design validation.

Commenting on the achievement, Cadence Product Management Director for Circuit Simulation Products Joy Han said, "This is a very exciting result and shows a disruptive and potentially game-changing approach to quantum computing. We hope to continue our collaboration with Equal1 long into the future."

22 Secret to Building Superconducting Quantum Computers With Massive Processing Power

by NIST

https://scitechdaily.com/secret-to-building-superconducting-quantum-computers-with-massive-processing-power/

The secret to building superconducting quantum computers with massive processing power may be an ordinary telecommunications technology – optical fiber.

Physicists at the NIST have measured and controlled a superconducting qubit using light-conducting fiber instead of metal electrical wires, paving the way to packing a million qubits into a quantum computer rather than just a few thousand. The demonstration is described in the March 25 issue of Nature.

Superconducting circuits are a leading technology for making quantum computers because they are reliable and easily mass produced. But these circuits must operate at cryogenic temperatures, and schemes for wiring them to room-temperature electronics are complex and prone to overheating the qubits. A universal quantum computer, capable of solving any type of problem, is expected to need about 1 million qubits. Conventional cryostats – supercold dilution refrigerators – with metal wiring can only support thousands at the most.

Optical fiber, the backbone of telecommunications networks, has a glass or plastic core that can carry a high volume of light signals without conducting heat. But superconducting quantum computers use microwave pulses to store and process information. So the light needs to be converted precisely to microwaves.

To solve this problem, NIST researchers combined the fiber with a few other standard components that convert, convey and measure light at the level of single particles, or photons, which could then be easily converted into microwaves. The system worked as well as metal wiring and maintained the qubit's fragile quantum states.

"I think this advance will have high impact because it combines two totally different technologies, photonics and superconducting qubits, to solve a very important problem," NIST physicist John Teufel said. "Optical fiber can also carry far more data in a much smaller volume than conventional cable."

Normally, researchers generate microwave pulses at room temperature and then deliver them through coaxial metal cables to cryogenically maintained superconducting qubits. The new NIST setup used an optical fiber instead of metal to guide light signals to cryogenic photodetectors that converted signals back to microwaves and delivered them to the qubit. For experimental comparison purposes, microwaves could be routed to the qubit through either the photonic link or a regular coaxial line.

The "transmon" qubit used in the fiber experiment was a device known as a Josephson junction embedded in a three-dimensional reservoir or cavity. This junction consists of two superconducting metals separated by an insulator. Under certain conditions an electrical current can cross the junction and may oscillate back and forth. By applying a certain microwave frequency, researchers can drive the qubit between low-energy and excited states (1 or 0 in digital computing). These states are based on the number of Cooper pairs – bound pairs of electrons with opposite properties – that have "tunneled" across the junction.

The NIST team conducted two types of experiments, using the photonic link to generate microwave pulses that either measured or controlled the quantum state of the qubit. The method is based on two relationships: The frequency at which microwaves naturally bounce back and forth in the cavity, called

the resonance frequency, depends on the qubit state. And the frequency at which the qubit switches states depends on the number of photons in the cavity.

Researchers generally started the experiments with a microwave generator. To control the qubit's quantum state, devices called electro-optic modulators converted microwaves to higher optical frequencies. These light signals streamed through optical fiber from room temperature to 4 kelvins (minus 269° C or minus 452° F) down to 20 millikelvins (thousandths of a kelvin), where they landed in high-speed semiconductor photodetectors, which converted the light signals back to microwaves that were then sent to the quantum circuit.

In these experiments, researchers sent signals to the qubit at its natural resonance frequency, to put it into the desired quantum state. The qubit oscillated between its ground and excited states when there was adequate laser power.

To measure the qubit's state, researchers used an infrared laser to launch light at a specific power level through the modulators, fiber and photodetectors to measure the cavity's resonance frequency.

Researchers first started the qubit oscillating, with the laser power suppressed, and then used the photonic link to send a weak microwave pulse to the cavity. The cavity frequency accurately indicated the qubit's state 98% of the time, the same accuracy as obtained using the regular coaxial line.

The researchers envision a quantum processor in which light in optical fibers transmits signals to and from the qubits, with each fiber having the capacity to carry thousands of signals to and from the qubit.

13 May 2021

23 NIST Releases Tips and Tactics for Dealing With Ransomware

by Chad Boutin

https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware

Used in cyberattacks that can paralyze organizations, ransomware is malicious software that encrypts a computer system's data and demands payment to restore access. To help organizations protect against ransomware attacks and recover from them if they happen, the National Institute of Standards and Technology (NIST) has published an infographic offering a series of simple tips and tactics.

NIST's advice includes:

- **Use antivirus software at all times** – and make sure it's set up to automatically scan your emails and removable media (e.g., flash drives) for ransomware and other malware.
- **Keep all computers fully patched with security updates.**
- **Use security products or services that block access to known ransomware sites** on the internet.
- **Configure operating systems or use third-party software to allow only authorized applications** to run on computers, thus preventing ransomware from working.
- **Restrict or prohibit use of personally owned devices** on your organization's networks and for telework or remote access unless you're taking extra steps to assure security.

NIST also advises users to follow these tips for their work computers:

- **Use standard user accounts** instead of accounts with administrative privileges whenever possible.
- **Avoid using personal applications and websites**, such as email, chat and social media, on work computers.
- **Avoid opening files, clicking on links, etc. from unknown sources** without first checking them for suspicious content. For example, you can run an antivirus scan on a file, and inspect links carefully.

Unfortunately, even with protective measures in place, eventually a ransomware attack may still succeed. Organizations can prepare for this by taking steps to ensure that their information will not be corrupted or lost, and that normal operations can resume quickly.

NIST recommends that organizations follow these steps to accelerate their recovery:

- **Develop and implement an incident recovery plan** with defined roles and strategies for decision making.
- **Carefully plan, implement and test a data backup and restoration strategy.** It's important not only to have secure backups of all your important data, but also to make sure that backups are kept isolated so ransomware can't readily spread to them.
- **Maintain an up-to-date list of internal and external contacts** for ransomware attacks, including law enforcement.

NIST has also published a more detailed fact sheet on how to stay prepared against ransomware attacks. You can find this material and more on ransomware at the NIST and CISA websites. These materials were produced by staff members in NIST's Information Technology Laboratory and National Cybersecurity Center of Excellence.

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. NIST is a nonregulatory agency of the U.S. Department of Commerce.

24 Quantum computing: Intel's cryogenic chip shows it can control qubits even in a deep freeze

by Daphne Leprince-Ringuet

https://www.zdnet.com/google-amp/article/quantum-computing-intels-cryogenic-chip-shows-it-can-control-qubits-even-in-a-deep-freeze/#amp_tf=From%20%251%24s&aoh=16211190162561&csi=0&referrer=https%3A%2F%2Fwww.google.com

Intel's quantum computing efforts are starting to show tangible results: two years after the company first unveiled its Horse Ridge cryogenic control chip, researchers have demonstrated that the technology is delivering on its original promise, and paving the way for quantum computers to become more practical.

Practicality, in effect, is not quantum devices' most remarkable trait. In their current format, quantum computers rely on quantum chips that need to be cooled down to extreme temperatures, in order to exert better control over the fragile qubits on the processor. Typically, qubits operate at 20 millikelvin, or about -273 degrees Celsius – temperatures that are even colder than outer space.

But to interact with the qubits, whether to control their behavior or read their state, flesh-and-bone scientists work in room-temperature environments, with room-temperature instruments. And since control electronics struggle to perform well at cryogenic temperatures, each qubit has to be linked to the instruments with a single wire.

It's easy to see why the set-up might become problematic as scientists contemplate the possibility of scaling up quantum computers to millions of qubits. This hurdle has become known as the "wiring bottleneck".

This is why, a few years ago, Intel teamed up with QuTech – a collaboration between Delft University of Technology and the Netherlands Organization for Applied Scientific Research – to work on another approach to the problem.

It took the form of a new control chip designed to withstand the cold and operate as close as possible to the quantum processor, which Intel unveiled for the first time in 2019. The device was named Horse Ridge – a reference to the coldest place in Oregon, which is also the state where the Intel lab resides.

Horse Ridge was built on Intel's 22-nanometer FinFET Low Power technology, and was presented as a potential way to bring key control functions for quantum computer operations directly into the cryogenic refrigerator, closer to the qubits themselves.

The underlying premise was that, if Horse Ridge could achieve the same level of control as room-temperature instruments, then the wiring bottleneck could be significantly reduced.

Horse Ridge was subsequently tweaked, and a second generation of the chip was showcased last year; but now, for the first time, Intel's researchers have demonstrated that the technology is as capable of controlling qubits as its room-temperature-based equivalents.

The research team used Horse Ridge to run a two-qubit algorithm called the Deutsch-Jozsa algorithm, and found that the cryogenic chip performed well despite the cold environment, and achieved control of the qubits with a same level of fidelity (99.7%) as room-temperature electronics.

"Our research results, driven in partnership with QuTech, quantitatively prove that our cryogenic controller, Horse Ridge, can achieve the same high-fidelity results as room-temperature electronics while controlling multiple silicon qubits," said Stefano Pellerano, principal engineer at Intel Labs.

Horse Ridge is a silicon-based CMOS chip, and as such was designed with a technology similar to that used in conventional microprocessors. The device was adapted to ensure the right operation even at cryogenic temperatures, which enables the chip to manipulate the state of qubits thanks to radio frequency pulses.

The qubits manipulated by Horse Ridge are also silicon-based, contrary to the type of qubits that can be found, for example, in IBM or Google's quantum computers, which are superconducting qubits. While Intel initially pursued both approaches – superconducting as well as silicon qubits – the company's recent efforts have ramped up in the latter.

This is because researchers are increasingly acknowledging that building quantum computers with techniques that are similar in nature to those used to produce most modern-day electronics could come with huge advantages when it comes to scaling the technology.

What's more: with both qubits and the controller chip fabricated in silicon, Intel's researchers are hoping that it may be possible to one day fully integrate them both together in one die or package. This would greatly simplify the wiring challenge of quantum and enable strides in quantum scalability.

"These innovations pave the way for fully integrating quantum control chips with the quantum processor in the future, lifting a major roadblock in quantum scaling," said Pellerano.

With these new results, Intel is cementing the company's position in the fast-evolving quantum ecosystem. While much of the focus remains on the qubits themselves, and on improving quantum processors, the Santa Clara giant has established that it is adopting a different course of action, instead working on developing the interconnects and control electronics that will create a quantum stack.

Integrating those systems, according to Intel, will be an important piece of the puzzle to achieve quantum practicality.

12 May 2021

25 UK crypto startup heads to Cayman Islands, Nasdaq, in $1.4bn SPAC deal

by Nick Flaherty

https://www.eenewseurope.com/news/uk-crypto-startup-heads-cayman-islands-nasdaq-14bn-spac-deal

The deal values Arqit at $1.4bn (€1.16bn) and raises $400m (€330m) for the development and launch of two satellites by 2023. These satellites will use its post-quantum encryption technology called QuantumCloud that the company says can protect communications links of any networked device secure against current and future forms of hacking, even from a quantum computer.

The deal with Centricus Acquisition Corp includes current business partners Virgin Orbit and Sumitomo, and Centricus sponsor Heritage Group. The merged company will be called Arqit Quantum Inc and willl be headquartered in the Cayman Islands with a listing on the NASDAQ stock exchange in the US. The company says its 'operatonal HQ' will remainin the UK.

Arqit has developed a way to create more secure symmetric keys when they are needed, at scale, securely, at any kind of end point device and in groups of any size. Current customers include the UK Government, the European Space Agency, BT, and Sumitomo. Verizon, BP, Northrop Grumman and Iridium are currently testing the use of Arqit's technologies in different ways.

"Arqit's business combination transaction represents a huge moment for the UK spacetech ecosystem," said James Bruegger, Chief Investment Officer at Seraphim Capital. "Arqit will be the first UK SpaceTech company to enter into a business combination transaction with a US publicly listed SPAC, in less than 5 years since its inception. Arqit is an excellent showcase for the UK's ability to produce world-leading companies in cutting edge areas such as quantum cybersecurity technology and Spacetech."

SPAC deals have become increasingly popular, with UK electric vehicle maker Arrival and Dublin-registered GaN chip maker Navitas both signed deals in the last month.

"Our research indicates that the SpaceTech industry has become one of the most sought-after markets for SPAC mergers," said Bruegger at Seraphim, which backed Arqit as well as ICeye in Finland and AT&S. "By the first quarter of 2021, 11 space-related companies have already announced their intention

to undertake transactions with SPACs. The industry finds itself at a watershed moment, and the transformative potential of SpaceTech is now accepted within the investment community, with SPAC transactions as the main means of accelerating their ability to access the capital required to realise their visions."

"Having first backed Arqit in its seed round in 2018, Seraphim Capital has invested in every round since and are proud to have supported Arqit's journey to become one of the most exciting cybersecurity companies in the world," he said.

Arqit's QuantumCloud puts a small software agent at any end point device. This software creates an unlimited number of symmetric keys with partner devices. The system currently uses source keys which are originated in data centres, however by 2023 it plans to launch two quantum satellites to assume that role.

Those satellites will use a new quantum protocol developed by Arqit as the backbone of secure keys within data centres all over the world. This would allow a user to create an infinite number of symmetric key pairs, in groups as large as are needed. Keys are never "delivered", so they cannot be intercepted. They are created at the end points and therefore can never be known by third parties. They can be used only once if necessary and replaced frequently n a self-service basis, ,aking it easily scalable.

"The world needs simpler, stronger cyber security, and Arqit addresses that need. After four years of innovation in stealth mode by a world leading multi- disciplinary teams of scientists and engineers, we are ready to go to market," said David Williams, CEO of Arqit. "This technology is important and we need to take it to hyperscale as quickly as possible, because the problems we solve are problems for everyone. The capital from this transaction will enable us to develop critical relationships with existing and new customers and fully scale our platform as a service with a balance sheet which gives us speed, momentum and the resilience to deliver on our commitments to customers for the long term."

"This transaction will give Arqit the ability to establish itself as a leader in the encryption space – the prospect of the threat from quantum computing will serve to accelerate the broad adoption of Arqit technology," said Garth Ritchie, CEO of of the SPAC vehicle Centricus. "This is a deep tech company which is many years ahead of the market. Arqit has protected its IP by remaining in stealth mode whilst filing over 1,000 claims on more than a dozen patent applications. It is thanks to funding from the British Government and its VC partners that Arqit is now ready to commercialise and scale its product suite; this will complement an already strong cohort of launch customers. The executive and advisory team are a 'transatlantic who's who' of relevant cybersecurity, space and military experience – this team also enjoys peerless access to relevant enterprise customers."

26 16 Companies Developing Quantum Algorithms

by James Dargan

https://thequantumdaily.com/2021/05/12/16-companies-developing-quantum-algorithms/

A Background to Quantum Algorithms

It is generally regarded that 1981 was the year quantum computing first appeared to the world. The Nobel Laureate Richard Feynman, a quantum visionary, had given a seminal speech at the First Conference on the Physics of Computation, organized in collaboration with MIT and IBM. In the speech, Feynman identified that it would be impossible for a classical computer to simulate quantum mechanical processes.

To do it, he proposed, a completely new kind of computer would be required, one that was aligned to the laws of quantum mechanics.

Unfortunately, a classical computer is inadequate at dealing with this as the exponential growth of data in a quantum system is far beyond its limits utilizing sub-exponential space and time complexity. A quantum computer, however – based on a quantum system that makes use of the non-classical properties – can process exponentially large amounts of data in only polynomial time. This is the uniqueness of the system.

With such a show of computational force using quantum mechanics, there are several fields that can benefit outside the remit of Newtonian mechanics. These include, but are not exclusive to, mathematics, cryptography and information theory.

Of all the buildouts realized from quantum information theory and computation, it is a paper by professor of applied mathematics at MIT Peter Shor which is the most influential. Shor's algorithm, first published in 1997, is an immense achievement of human intellectual power. The quantum algorithm, then, performs prime factorization of integers in polynomial time.

But what does this actually achieve?

In a word, it gives us the power to exponentially speed up and even beat the fastest of algorithms built from classical systems. As of yet, there are no known classical algorithms that can successfully factor integers into prime numbers. By using quantum algorithms like Shor's, it is possible to do things that previously were thought impossible, like breaking public-key cryptographic systems like RSA, which rely on classical algorithms' inability to crack them.

Since Shor's algorithm came into being more than twenty years ago, there have been many quantum algorithms devised for use on the ever-expanding quantum computing hardware that is being developed by the likes of D-Wave Systems, Google, IBM and Microsoft.

And that, no doubt, is set to continue as we move into this next decade.

The quantum decade.

With that in mind, TQD thought it time to put out its own list of the players in the quantum computing industry that are developing quantum algorithms to service the growing ecosystem, based on the wealth of data available at The Quantum Insider (TQI), our very own data platform.

I have omitted all the large public companies, for one, though there are still several big private players represented. Why? Well, it's always good to give the smaller fish a chance, isn't it?

(i) **1QBit**

(ii) **Algorithmiq**

(iii) **Cambridge Quantum Computing**

(iv) **BEIT**

(v) **CLASSIQ**

(vi) **Entropica Labs**

(vii) **ExaQ.ai**

(viii) **HQS Quantum Simulations**

(ix) **Jij**

(x) **JoS Quantum**

(xi) **Ketita Labs**

(xii) **Phasecraft**

(xiii) **QunaSys**

(xiv) **Semicyber**

(xv) **Solid State AI**

(xvi) **Zapata Computing**

27 CINECA and D-Wave Expand Access to Quantum Computing in Italy

https://insidehpc.com/2021/05/cineca-and-d-wave-expand-access-to-quantum-computing-in-italy/#:~:text=BOLOGNA%2C%20ITALY%20and%20BURNABY%2C%20BC,%2C%20researchers%2C%3D%20and%20developers%20expandedhttps://www.research.ibm.com/blog/120x-quantum-speedup

CINECA, the Italian inter-university consortium and supercomputing center, and D-Wave Systems Inc., the quantum computing systems, software and services company, today announced a formal collaboration to offer Italian universities, researchers, and developers expanded access to practical quantum computing technology and resources through D-Wave's Leap quantum cloud service.

CINECA, which is made up of 69 Italian universities, 25 national research institutions, the Ministry of Education, and the Ministry of Universities and Research, will benefit from expanded, real-time access to the Leap quantum cloud service. This access includes D-Wave's hybrid quantum/classical solvers, which leverage both quantum solutions and best-in-class classical algorithms to run large-scale business-critical problems. With real-time access to quantum computers via the cloud, the Italian and international scientific community have the opportunity to further quantum education, publication, and R&D, while boosting the development of real-world quantum applications.

This collaboration aids the consortium's mission to support Italy's scientific community and improve quantum computing literacy and skills training for university partners. This, in turn, will benefit the larger public administration and private enterprise ecosystem. CINECA university members, such as the Polytechnic University of Milan, have already expressed interest in leveraging quantum computing to explore drug repurposing and development, natural disaster response and relief, and sustainability challenges such as decarbonization and energy production. As an example of the value of the collaboration, D-Wave and CINECA hosted a joint webinar on March 31st showcasing CINECA's work on molecular docking for drug discovery utilizing D-Wave's quantum system.

D-Wave will also provide cloud access via Leap to its latest generation quantum system, Advantage, which includes:

- **Updated Topology:** The topology in Advantage makes it the most connected of any commercial quantum system in the world. In the Advantage system, each qubit may connect to 15 other qubits, enabling the embedding of larger, more complex problems.
- **Increased Qubit Count:** Advantage includes more than 5000 qubits. More qubits and richer connectivity provide quantum programmers access to a larger, denser, and more powerful graph for building commercial quantum applications.
- **Greater Performance & Problem Size:** With the capacity to solve problems with up to 1 million variables, the hybrid solver service in Leap allows researchers to run large-scale, business-critical problems, expanding the complexity and more than doubling the size of problems that can run directly on the quantum processing unit (QPU).
- **Expansion of Hybrid Software & Tools in Leap:** The hybrid solver service, new solver classes, ease-of-use, automation, and new tools provide an even more powerful hybrid rapid development environment in Python for business-scale problems.
- **Ongoing Releases:** D-Wave continues to bring innovations to market with additional hybrid solvers, QPUs, and software updates through the cloud. Users can get started today with Advantage and the hybrid solver service, and will benefit from new components of the platform through Leap as they become available.

"We have enjoyed a long-standing relationship with the pioneering team at CINECA, which was one of the first non-profit consortiums to explore quantum computing with us," said Daniel Ley, SVP Global Sales, D-Wave. "Bringing quantum computing to the world requires more than just vendors alone. We need to continue to build a robust ecosystem of developers and researchers, innovative scientific institutions, cutting-edge academic organizations, and forward-thinking businesses to work together. CINECA is aligned with us in that mission and committed to helping their ecosystem build practical and applied quantum computing applications."

"At CINECA we are very happy to be part of this agreement with D-Wave. Quantum computing is a field that has been strongly emerging in recent years," said Sanzio Bassini, Head of the HPC Department at CINECA. "Its natural association with HPC, which CINECA has been dealing with for more than 50 years, makes the issue of high interest both for CINECA and for the entire ecosystem of universities and research institutions that it represents. Thanks to D-Wave for the collaboration. I have no doubt that it will be a wonderful experience for both parties."

"Thanks to the quantum team at CINECA we were able to start addressing part of our molecular docking problem using D-Wave's system," said Gianluca Palermo, Associate Professor at the Polytechnic University of Milan. "They supported us in the problem formulation such that it was manageable by the quantum solver, and in its deployment on the quantum machine. This is the key to educating a team with no prior experience and helping them evaluate the endless possibilities offered by quantum systems."

11 May 2021

28 QphoX invents the Quantum Modem as the future gateway to the quantum internet

by Rutger Huizenga

https://quantumdelta.nl/qphox-invents-the-quantum-modem-as-the-future-gateway-to-the-quantum-internet/

Quantum technology start-up QphoX has raised two million euros to launch its Quantum Modem™, a technology poised to have a major impact on the future of quantum computing. We spoke with co-founder Simon Gröblacher to learn more about his journey. He is the first founder to launch through the LightSpeed program by Quantum Delta NL, so we got his story on this special project too.

Quantum computing is widely regarded as the next big step forward in computing, allowing for certain complex problems to be solved that are not feasible with standard computers. This has the potential to transform what's possible in fields like cybersecurity, A.I., and drug development. To connect different quantum computers and have them exchange information, you need a quantum internet. Such a network will allow you to combine different quantum technologies, increase the combined computational power of the computers and bridge large distances using quantum communication channels.

The challenge however is finding a way for quantum computers to be able to start talking to each other. QphoX was started by Simon Gröblacher, Professor of Quantum Physics at TU Delft and physicists Robert Stockill and Frederick Hijazi, to tackle this problem. They developed the Quantum Modem™, a breakthrough device that will allow quantum computers to talk to one another by unlocking the potential of the 'quantum internet'.

"It's the missing link to enable quantum computers to exchange quantum information with one another over large distances", Simon explains. "We named it the Quantum Modem™ because it's really like a classical modem that connects computers together over the internet. We do the same in the quantum domain by converting an electrical quantum signal into an optical quantum signal."

Where some quantum companies take years to get off the ground, QphoX shot to prominence as their Quantum Modem™ quickly led to interest from major investors and eventually a two million euro seed funding ticket, in a funding round led by Quantonation, Speedinvest and High-Tech Gründerfonds, with participation from TU Delft.

"We couldn't have had a better start", Simon admits. "Before starting the company, we have built proof of concept devices in the lab, so we know it works. Thanks to this investment, we will be able to develop the QphoX Quantum Modem™ into a commercial product, combining the fields of quantum computing and quantum communications."

29 Germany to invest €2bn in building first quantum computer

by E&T editorial staff

https://eandt.theiet.org/content/articles/2021/05/germany-to-invest-2bn-in-building-first-quantum-computer/

The German government is to spend billions of euros to support the development of the country's first quantum computer and related technologies.

The announcement, reported by Reuters, was made by the economy and science ministries this week. The science ministry will contribute €1.1bn by 2025 to support R&D in quantum computing, while the economy ministry will contribute €878m to support the development of applications.

The German Aerospace Centre (DLR), the national aeronautics and space research centre, will receive the largest share of the funds (€720m). The funds will help it team up with industry – ranging from large companies to start-ups – in order to form two consortia for quantum computing.

"Quantum computing has the potential to revolutionise key industries of our economy," said Peter Altmaier, the economy minister, citing areas such as managing supply and demand and testing new active substances. "It's our goal that Germany will become one of the best players worldwide in the development and practical application of quantum computing."

Science minister Anja Karliczek added that the government aims to build a competitive quantum computer in five years while growing a network of companies to develop applications: "Today, we start the mission quantum computer 'Made in Germany' and now we are ready for take-off," she said.

The large state subsidies will need to be approved by the European Commission. It is unlikely to reject the proposals, having used its 2030 Digital Compass plan to urge member states to develop the bloc's first quantum computer (complexity not specified) in five years amid a wider effort to reduce reliance on non-European technologies.

In 2019, the UK government pledged to spend £153m in public funding on the domestic development of quantum computing.

Quantum computing involves the use of quantum phenomena such as superposition to carry out calculations. Quantum computers use quantum versions of bits (qubits); while bits can be either a 0 or a 1, a qubit can represent 0, 1, or any superposition of these two states. While quantum computers are in very early stages of development, they have the potential to exponentially expand computing power, transforming certain sectors such as cyber security and research.

Meanwhile, the DLR has partnered with Cambridge Quantum Computing to explore how quantum computing could help create improved simulations for battery development to assist future energy utilisation. DLR will use Cambridge Quantum Computing's algorithms to simulate a 1D lithium-ion battery cell, laying the foundation for simulations of complete battery cells with quantum computers, including full 3D models. DLR plans to render its quantum simulations using an IBM quantum computer.

30 IBM Quantum delivers 120x speedup of quantum workloads with Qiskit Runtime

https://www.research.ibm.com/blog/120x-quantum-speedup

We're pleased to announce that the team demonstrated a 120× speedup in simulating molecules thanks to a host of improvements, including the ability to run quantum programs entirely on the cloud with Qiskit Runtime.

Last fall, we made the ambitious promise to demonstrate a 100× speedup of quantum workloads in our IBM Quantum roadmap for scaling quantum technology. Today, we're pleased to announce that we didn't just meet that goal; we beat it. The team demonstrated a 120× speedup in simulating molecules thanks to a host of improvements, including the ability to run quantum programs entirely on the cloud with Qiskit Runtime.

Until now, we have mostly focused on the execution of quantum circuits, or sequences of quantum operations, on IBM Quantum systems. However, real applications also require substantial amounts of classical processing. We use the term quantum program to describe this mixture of quantum circuits and classical processing. Some quantum programs have thousands or even millions of interactions between quantum and classical. Therefore, it is critical to build systems that natively accelerate the execution of

quantum programs, and not just quantum circuits. Systems built to execute quantum programs need to have significantly larger effective capacities, and they require improvements across the stack, including cloud service design, system software, control hardware, and even quantum hardware.

Back in 2017, the IBM Quantum team demonstrated that a quantum computer could simulate the behavior of the lithium hydride molecule[1] – a preview of the kinds of applications we hope that quantum computers will tackle in the future. However, the process of modeling the LiH molecule would take 45 days with today's quantum computing services, as circuits repeatedly passed back-and-forth between a classical and quantum processor and introduced large latencies.

A host of improvements went into this feat. Algorithmic improvements reduced the number of iterations of the algorithm required to receive a final answer by two to 10 times. Improvements in system software removed around 17 seconds per iteration. Improved processor performance led to a 10× decrease in the number of shots, or repeated circuit runs, required by each iteration of the algorithm. And finally, improved control systems such as better readout and qubit reset performance reduced the amount of time per job execution (that is, execution of each batch of a few dozen circuits) from 1000 microseconds to 70 microseconds.

The final boost came from the introduction of the Qiskit Runtime – a containerized service for quantum computers. Rather than building up latencies as code passes between a user's device and the cloud-based quantum computer, developers can run their program in the Qiskit Runtime execution environment, where the IBM hybrid cloud handles the work for them. New software architectures and OpenShift Operators allow us to maximize the time spent computing, and minimize the time spent waiting.

We hope that this speedup will allow more developers to experiment with quantum applications in chemistry – and beyond. For example, the Qiskit Runtime will allow users to try out our powerful new quantum kernel alignment algorithm, which searches for an optimal quantum kernel with which to perform machine learning tasks. We recently used this algorithm to prove that quantum computers will demonstrate a rigorous speedup over classical computers for supervised machine learning.

The IBM Quantum team is committed to finding practical quantum computing use cases, and delivering them to the largest possible developer base. We hope that the Qiskit Runtime will allow users around the world to take full advantage of the 127 qubit IBM Quantum Eagle device slated for this year – or the 1121-qubit Condor device planned for 2023.

Qiskit Runtime is currently in beta for some members of the IBM Quantum Network.

31 The widely anticipated quantum internet breakthrough is finally here

by maija palmer

https://sifted.eu/articles/quantum-internet-breakthrough/

If you thought quantum computing was a leap forward, get ready for the next step: the quantum internet, where quantum machines can be linked to each other to create powerful networks of superfast computing power.

[1] This Nature cover story, Hardware-efficient Variational Quantum Eigensolver for Small Molecules and Quantum Magnets, also detailed the simulation of beryllium hydride.

The vision is now even closer to becoming reality. **QphoX**, a Delft University spinout, has created a quantum modem that can get these machines talking to each other. It plans to be the first to take it out of the research lab and turn it into a commercial project – and has raised €2m seed round to build the company.

It is the next big step in quantum computing. Today's biggest quantum computers have less than 100 qubits, but scientists say that the machines will need at least 1k qubits to be truly commercially useful. Scaling up the computers themselves will take time, but a quantum internet could connect smaller machines to get to 1k+ qubits faster.

"Scaling a quantum computer even beyond 100 qubits is hard at the moment, but you could link 10 together to get 1k," says Simon Gröblacher, CEO and cofounder of QphoX. Gröblacher says they expect to have a working modem ready for customers to test within two years.

The seed funding round was led by Quantonation, Speedinvest and High-Tech Gründerfonds, with participation from TU Delft.

"The €2m is earmarked for moving the technology from the university research lab to a company, and hiring additional people. We need to mature the technology and create proper software around it," said Gröblacher. QphoX has recently expanded from just its three cofounders to a team of six, and is looking to recruit a handful more people.

The company is currently in discussions to run pilots with a number of quantum computer companies.

"That was one of the things that reassured our investors, the positive feedback from potential customers that this isn't some random idea, they could see there is a real need for this solution," Gröblacher said.

The modem is designed in the first instance to work with machines using superconducting qubits, but will in theory also connect to other types of quantum computer, such as those based on spin or topological qubits – anything that works with microwave frequencies.

The secret is in being able to convert the microwave frequency readouts from a quantum processor and turn these into optical signals that can be transmitted down optical fibre networks. This all happens on a small chip that can sit just outside the quantum computing cryostat (the freezer that keeps the qubits at temperatures close to absolute zero).

It would be able to not only link quantum processors together but also link processors to quantum memory systems and other parts of the computer system.

"It is hard to see a winner-takes-all company in quantum computing – it is hard enough to build a quantum processor, and so it is likely you will have different companies developing different parts. They will need to be able to talk to each other," said Gröblacher.

Olaf Joeressen, Senior Investment Manager at High-Tech Gründerfonds, said: "The Qphox team is on a journey to make quantum computing scalable and provide real world impact soon based on their groundbreaking research. In our view, the quantum-transducer from QphoX has the potential to become an indispensable component of the quantum computing architecture of the future."

One of the main goals for the QphoX team now is to get the conversion from microwave to optical to be more efficient.

"We are clear on how to do it, it is just a case of engineering it and putting it together," said Gröblacher.

While a number of research groups are working on quantum modem concepts, QphoX believes it will be the first to commercialise the technology.

09 May 2021

32 Complex Shapes of Photons for Fast Photonic Quantum Computations and Safe Data Transfer

by tampere university

https://scitechdaily.com/complex-shapes-of-photons-for-fast-photonic-quantum-computations-and-safe-data-transfer/

As the digital revolution has now become mainstream, quantum computing and quantum communication are rising in the consciousness of the field. The enhanced measurement technologies enabled by quantum phenomena, and the possibility of scientific progress using new methods, are of particular interest to researchers around the world.

Recently two researchers at Tampere University, Assistant Professor Robert Fickler and Doctoral Researcher Markus Hiekkamäki, demonstrated that two-photon interference can be controlled in a near-perfect way using the spatial shape of the photon. Their findings were recently published in the prestigious journal Physical Review Letters.

"Our report shows how a complex light-shaping method can be used to make two quanta of light interfere with each other in a novel and easily tuneable way," explains Markus Hiekkamäki.

Single photons (units of light) can have highly complex shapes that are known to be beneficial for quantum technologies such as quantum cryptography, super-sensitive measurements, or quantum-enhanced computational tasks. To make use of these so-called structured photons, it is crucial to make them interfere with other photons.

"One crucial task in essentially all quantum technological applications is improving the ability to manipulate quantum states in a more complex and reliable way. In photonic quantum technologies, this task involves changing the properties of a single photon as well as interfering multiple photons with each other;" says Robert Fickler, who leads the Experimental Quantum Optics group at the university.

Linear optics bring promising solutions to quantum communications

The demonstrated development is especially interesting from the point of view of high-dimensional quantum information science, where more than a single bit of quantum information is used per carrier. These more complex quantum states not only allow the encoding of more information onto a single photon but are also known to be more noise-resistant in various settings.

The method presented by the research duo holds promise for building new types of linear optical networks. This paves the way for novel schemes of photonic quantum-enhanced computing.

"Our experimental demonstration of bunching two photons into multiple complex spatial shapes is a crucial next step for applying structured photons to various quantum metrological and informational tasks," continues Markus Hiekkamäki.

The researchers now aim at utilizing the method for developing new quantum-enhanced sensing techniques, while exploring more complex spatial structures of photons and developing new approaches for computational systems using quantum states.

"We hope that these results inspire more research into the fundamental limits of photon shaping. Our findings might also trigger the development of new quantum technologies, e.g. improved noise-tolerant quantum communication or innovative quantum computation schemes, that benefit from such high-dimensional photonic quantum states," adds Robert Fickler.

33 Chinese team designs 62-qubit quantum processor with world's largest number of superconducting qubits

by Wan Lin

https://www.globaltimes.cn/page/202105/1222944.shtml

A Chinese research team has successfully designed a 62-qubit programmable superconducting quantum processor, naming it ***Zu Chongzhi*** after the noted 5th century Chinese mathematician and astronomer. The computer contains the largest number of superconducting qubits so far in the world, and achieved two-dimensional programmable quantum walks on the system, a major milestone in the field.

Experts said the study pushes the possibility of universal quantum computing through a two-dimensional quantum walk a big step forward.

The study was conducted by a research team from the University of Science and Technology of China (USTC), and was published Friday in Science magazine, one of the top academic journals in the world.

The team designed and produced an 8×8 two-dimensional square superconducting qubit array composed of 62 functional qubits in the study, and used this device to demonstrate high fidelity single and two particle quantum walks, according to the team.

Such a device can achieve universal quantum computing, which means that any computing task can be done in this manner, Yuan Lanfeng, a research fellow at the Hefei National Laboratory for Physical Sciences at the Microscale of the USTC, told the Global Times on Sunday.

"It is just like one or two particles randomly moving on an 8×8 chess board. Such random quantum walks can achieve anything that quantum computing can do, which is amazing," he said.

The work was an essential milestone, bringing future larger scale quantum applications closer to realization on noisy intermediate-scale quantum processors, said the team in the article.

The development of quantum computers, one of the major challenges in the forefront of science and technology in the world, has become the focus of competition among countries globally.

US technology giant Google announced a 53-qubit programmable superconducting processor, named Sycamore, in October 2019, and claimed "quantum supremacy," a term to describe the point at which quantum computers solve problems beyond the ability of non-quantum, or classical computers.

Yuan said the 62-qubit *Zu Chongzhi* processor at least showed that China is at the same level as its US counterparts in the field of superconducting quantum computing.

Pan Jianwei, a renowned Chinese quantum physicist who led the research team for *Zu Chongzhi*, also developed Jiuzhang, a new light-based quantum computer prototype with his team, and they demonstrated "quantum advantage," the second time a quantum algorithm claimed to achieve this feat in the world, after the first claimed by Google's Sycamore in 2019.

Unlike the Jiuzhang processor, which conducts only one task – finding solutions to the boson-sampling

problem – the new *Zu Chongzhi* processor has the potential to do "everything," even though it may not excel quantum computers for any specific task, Yuan said, adding that the photonic technology that the Jiuzhang processor uses and the superconducting technology that Zu Chongzhi uses are two mainstream technical routes that quantum processors employ.

Quantum computers have superfast parallel computing power, and hold the promise of exponentially accelerating the ability of classical computers in solving important social and economic problems, such as cryptography, big data optimization, material design and drug analysis, through specific algorithms.

Superconducting quantum computing is among the most promising candidates for scalable quantum computing. Its core objective is to synchronously increase the number of integrated qubits and improve the performance of superconducting qubits, so as to achieve exponential acceleration in the processing speed of specific problems, and finally apply it in practice.

The new *Zu Chongzhi* superconducting quantum computer can be applied to transportation planning, allowing for major optimization of traffic flows in a city, Yuan said.

It can also be used in the field of pharmaceuticals, quickly selecting the most promising combination of drug molecules from all available drug molecule candidates, he added, noting that people have high hopes for putting superconducting quantum computers into use in the pharmaceutical sector in five years.

The two-dimensional programmable quantum walks based on quantum computing have potential applications in quantum search algorithms, general quantum computing and other fields, and will be an important direction of subsequent development, according to a statement from the USTC on Saturday.

34 10 Companies Providing Full-Stack Quantum Solutions

by James Dargan

https://www.thequantumdaily.com/2021/05/09/10-companies-providing-full-stack-quantum-solutions/

For most startups participating in the quantum computing (QC) ecosystem, the best way to compete commercially is to develop novel software, start a consultancy or other similar service-based platforms. Software, as an example, is naturally much cheaper to develop than the obvious cost-heavy manufacturing of hardware products.

Hardware and full-stack services in quantum, unsurprisingly then, seem to be the domain of the big players like Microsoft and a few that are mentioned below. However, there are some companies with neither the financial clout nor the name of a Microsoft that are going full-stack, too.

TQD will now list, in alphabetical order, ten of those which are set to change the game in this sphere. They are – thank goodness – spread across the globe, from North America to Europe to China.

(i) Alibaba Quantum Lab (China)

(ii) Alpine Quantum Technologies (Austria)

(iii) D-Wave Systems (Canada)

(iv) Google AI Quantum (US)

(v) IBM (US)

(vi) IQM (Finland)

(vii) Origin Quantum (China)

(viii) Oxford Quantum Circuits (UK)

(ix) Quantum Circuits, Inc (US)

(x) Xanadu (Canada)

35 US pipeline company halts operations after cyberattack

https://indianexpress.com/article/world/us-pipeline-company-halts-operations-after-cyberattack-7307789/

The operator of a major pipeline system that transports fuel across the East Coast said Saturday that it had been victimised by a ransomware attack and that it had halted all pipeline operations to deal with the threat.

Colonial Pipeline did not say what was demanded or by whom, but ransomware attacks are typically carried out by criminal hackers who seize data and demand a large payment in order to release it.

The attack on a pipeline operator, which says it delivers roughly 45% of all fuel consumed on the East Coast, underscored again the vulnerabilities of critical infrastructure to cyberattacks both by criminal hackers and US adversaries.

It presents a new challenge for an administration still grappling with its response to major hacks from months ago, including a massive breach of government agencies and corporations for which the US sanctioned Russia last month.

In this case, Colonial Pipeline said the ransomware attack Friday affected some of its information technology systems and that the company moved "proactively" to take certain systems online, halting pipeline operations.

The Alpharetta, Georgia-based company transports gasoline, diesel, jet fuel and home heating oil from refineries primarily located on the Gulf Coast through pipelines running from Texas to New Jersey.

The company said it hired a cybersecurity firm to investigate the nature and scope of the attack and has also contacted law enforcement and federal agencies.

In a statement late Friday, Colonial Pipeline said it was "taking steps to understand and resolve this issue," focused primarily on "the safe and efficient restoration of our service and our efforts to return to normal operation."

It said it was "working diligently to address this matter and to minimise disruption to our customers and those who rely on Colonial Pipeline."

While there have long been fears about US adversaries disrupting American energy suppliers, ransomware attacks by criminal syndicates are much more common and have been soaring lately.

Oil analyst Andy Lipow said the impact of the attack on fuel supplies and prices depends on how long the pipeline is down. An outage of one or two days would be minimal, he said, but an outage of five or six days could cause shortages and price hikes, particularly in an area stretching from central Alabama to the Washington, D.C., area.

Lipow said a key concern about a lengthy delay would be the supply of jet fuel needed to keep major airports operating, like those in Atlanta and Charlotte, North Carolina.

A leading expert in industrial control systems, Dragos CEO Robert Lee, said systems such as those that directly manage the pipeline's operation have been increasingly connected to computer networks in the past decade.

But critical infrastructure companies in the energy and electricity industries also tend to have invested more in cybersecurity than other sectors. If Colonial's shutdown was mostly precautionary – and it detected the ransomware attack early and was well-prepared – the impact may not be great.

Ransomware scrambles a victim organization's data with encryption. The criminals leave instructions on infected computers for how to negotiate ransom payments and, once paid, provide software decryption keys.

Mike Chapple, teaching professor of IT, analytics and operations at the University of Notre Dame's Mendoza College of Business and a former computer scientist with the National Security Agency, said systems that control pipelines should not be connected to the internet and vulnerable to cyber intrusions.

"The attacks were extremely sophisticated and they were able to defeat some pretty sophisticated security controls, or the right degree of security controls weren't in place," Chapple said.

Brian Bethune, a professor of applied economics at Boston College, also said the impact on consumer prices should be short-lived as long as the shutdown does not last for more than a week or two. "But it is an indication of how vulnerable our infrastructure is to these kinds of cyberattacks," he said.

Bethune noted the shutdown is occurring at a time when energy prices have already been rising as the economy reopens further as pandemic restrictions are lifted. According to the AAA auto club, the national average for a gallon of regular gasoline has increased by four cents since Monday to $2.94.

Colonial Pipeline said it transports more than 100 million gallons of fuel daily, through a pipeline system spanning more than 5,500 miles.

The FBI and the White House's National Security Council did not immediately return messages seeking comment. The federal Cybersecurity Infrastructure and Security Agency referred questions about the incident to the company.

A hacker's botched attempt to poison the water supply of a small Florida city raised alarms about how vulnerable the nation's critical infrastructure may be to attacks by more sophisticated intruders.

Anne Neuberger, the Biden administration's deputy national security adviser for cybersecurity and emerging technology, said in an interview with The Associated Press in April that the government was undertaking a new effort to help electric utilities, water districts and other critical industries protect against potentially damaging cyberattacks. She said the goal was to ensure that control systems serving 50,000 or more Americans have the core technology to detect and block malicious cyber activity.

Since then, the White House has announced a 100-day initiative aimed at protecting the country's electricity system from cyberattacks by encouraging owners and operators of power plants and electric utilities to improve their capabilities for identifying cyber threats to their networks. It includes concrete milestones for them to put technologies into use so they can spot and respond to intrusions in real time. The Justice Department has also announced a new task force dedicated to countering ransomware attacks.

08 May 2021

36 evolutionQ Introduces Quantum Delivery Network (QDN) to Help Extend QKD Networks

https://quantumcomputingreport.com/evolutionq-introduces-quantum-delivery-network-qdn-to-help-extend-qkd-networks/

The software product from evolutionQ is called BasejumpQDN and is designed to help users overcome the limitations of QKD networks. Chief among these is the distance limitation inherent in fiber optic cables due to signal loss. While classical optical communications networks can solve this by installing classical repeaters every few hundred kilometers, the No Cloning theorem for quantum qubits prevents one from copying qubits so creating these types of repeaters is more difficult. BasejumpQDN solves this problem by allowing a user to create a Trusted Node between quantum links that will allow a network to expand beyond the distance limitations. BasejumpQDN will also allow a user to set up a demonstration or simulated QKD network even without actual QKD devices to allow organizations to experiment with this technology and develop business cases before installing a full network.

07 May 2021

37 Capturing a single photon of light: Harnessing quantum's 'noise problem'

by Raytheon BBN Technologies

https://phys.org/news/2021-05-capturing-photon-harnessing-quantum-noise.html

Scientists at Raytheon BBN Technologies have developed a new way to detect a single photon, or particle of light – a development with big applications for sensors, communications and exponentially more powerful quantum computer processors.

The team has published its work, which centers on the use of a component called a Josephson junction, in the academic journal Science. The discovery builds on the same team's previous research into a microwave radiation detector 100,000 times more sensitive than existing systems.

"A Josephson junction in quantum computing is analogous to a transistor for modern electronics, so they are super important," said Kin Chung Fong, a quantum information processing scientist at Raytheon BBN Technologies and a research associate at Harvard University. "Our new device enables this basic unit in quantum computing to communicate through as little as one photon. It will improve the speed in the communication and can make quantum networking and sensing possible."

Researchers and labs around the world have started building larger quantum computers, seeking to unlock the promise of faster processing.

"In theory quantum computers can take over where traditional computers would run out of processing power," said Brad Tousley, president of Raytheon BBN Technologies. "Quantum computers are particularly good at solving critical optimization problems. One example would be for a computer-aided design of a large system like an aircraft. Quantum computing allows for more finite analysis of something like a wing shape than ever before. Fundamental everyday processing optimization is the first problem we'd like to tackle with quantum computing."

The technical limitation has been the background noise that causes qubits to lose memory, creating errors in the processing. While other researchers see the noise as problem, Fong and his team see opportunity.

Their method works a little like a highway, where superconducting charges play the role of cars. In principle, they can move very fast without bumping into each other. Background noise is like a broken-down car in the center lane – it breaks the flow of traffic.

"The interruption could destroy the data in quantum computing applications," Fong said. "However, we can utilize this same phenomenon to detect a single photon, allowing the traffic to continue to speed along."

The discovery is part of a research effort at Raytheon BBN Technologies, a subsidiary of Raytheon Intelligence & Space. Raytheon BBN has been providing advanced technology research and development for more than 70 years, often serving as a crucial link between the military and researchers at universities. As an example, it was one of the first nodes in the ARPANET, the precursor of the internet funded by the Defense Advanced Research Projects Agency, or DARPA. Scientists at Raytheon BBN work in broad-reaching portfolios, while quantum engineering and computing continues to show promise for next-generation capabilities.

"This discovery is going to open up quantum processors to be connected like never before," Tousley said. "The next step is characterizing performance and scaling up to more than one device in parallel or linking multiple devices."

The Raytheon BBN team believe they have the systems engineering expertise to take this basic research to more practical applications.

"We've filled a technological void with the first Josephson junction to detect a single photon," said Fong. "It's an enabling technology for networking, communication and computation. We are really just scratching the surface."

38 Thales and Senetas Team to Offer a Post Quantum Cryptography Solution

https://quantumcomputingreport.com/thales-and-senetas-team-to-offer-a-post-quantum-cryptography-solution/

French multinational Thales and Australian company Senetas have announced a post quantum cryptography solution for enterprises and governments around the world. Although most experts believe it will still be somewhere between 10 an 30 years before a powerful enough quantum computer is created that can factor a large semi-prime number and hence break the RSA encryption code used for key exchange, there is a concern about an attack that we call "**Harvest Now, Decrypt Later**". The "Harvest Now, Decrypt Later" attack could be utilized to collect data that has the characteristics of both high value as well as high shelf life. This could include things like medical records or the design plans for a new military aircraft or other things that would still be useful to know at a time well in the future. The attacker will collect the encrypted data today on a hard drive and hold it for many years until they obtain a large quantum computer and then use it to decrypt and uncover the data.

So for this reason, some organizations are already starting to put into place quantum resistant encryption capabilities to prevent this type of attack. The U.S. NIST agency has been running a Post

Quantum Cryptography standardization competition for several years now and is currently in Round 3 with 7 finalists and 8 alternatives. They are anticipating releasing their final selections in the next year or two.

So even though the NIST selection is not fully completed yet, The Thales/Senetas solution is already supporting the finalist algorithms and will transition to the final selection once that is made. They will adhere to standards from both NIST and the European Telecommunications Standards Institute in their products.

39 Cybersecurity warning: Russian hackers are targeting these vulnerabilities, so patch now

by Danny Palmer

https://www.zdnet.com/article/cybersecurity-warning-russian-hackers-are-targeting-these-vulnerabilities-so-patch-now/

Russian cyber attacks are being deployed with new techniques – including exploiting vulnerabilities like the recent Microsoft Exchange zero-days – as its hackers continue to target governments, organisations and energy providers around the world.

A joint advisory by, the US Department for Homeland Security's Cybersecurity Infrastructure Security Agency (CISA), FBI and the National Security Agency (NSA),as well as the UK National Cyber Security Centre looks to warn organisations about updated Tactics, Techniques and Procedures (TTPs) used by Russia's foreign intelligence service, the SVR – a group also known by cybersecurity researchers as APT29, Cozy Bear, and The Dukes.

It comes after cybersecurity agencies in the US and the UK attributed the SolarWinds attack to Russia's civilian foreign intelligence service, as well as several campaigns targeting Covid-19 vaccine developers.

"The SVR is a technologically sophisticated and highly capable cyber actor. It has developed capabilities to target organisations globally, including in the UK, US, Europe, NATO member states and Russia's neighbours," said the alert.

The advisory warns that Russian cyber attackers have updated their techniques and procedures in an effort to infiltrate networks and avoid detection, especially when some organisations have attempted to adjust their defences after previous alerts about cyber threats.

This includes the attackers using open source tool Sliver as a means of maintaining access to compromised networks and making use of numerous vulnerabilities, including vulnerabilities in Microsoft Exchange.

Sliver is an open source red team tool, a tool used by penetration testers when legally and legitimately testing network security, but in this case is being abused to consolidate access to networks compromised with WellMess and WellMail, custom malware associated with SVR attacks.

Although the paper warns that this isn't necessarily a full list, other vulnerabilities – all of which have security patches available – used by Russian attackers, include:

- CVE-2018-13379 FortiGate
- CVE-2019-1653 Cisco router

- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-9670 Zimbra
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2019-7609 Kibana
- CVE-2020-4006 VMWare
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-21972 VMWare vSphere

The attackers are also targeting mail servers as part of their attacks as they're useful staging posts to acquire administrator rights and the ability to further network information and access, be it for gaining a better understanding of the network, or a direct effort to steal information.

But despite the often advanced nature of the attacks, the paper by US and UK cybersecurity authorities says that "following basic cyber security principles will make it harder for even sophisticated actors to compromise target networks".

This includes applying security patches promptly so no cyber attackers – cyber criminal or nation-state backed operative – can exploit known vulnerabilities as a means of entering or maintaining persistence on the network.

Guidance by the NCSC also suggests using multi-factor authentication to help protect the network from attack, particularly if passwords have been compromised.

40 New Boost in Quantum Technologies

by Karine

https://thequantumhubs.com/new-boost-in-quantum-technologies/

Researchers at the University of Stuttgart were able to detect qubits in two-dimensional materials for the first time.

Quantum computers or quantum sensors consist of materials that are completely different to their classical predecessors. These materials are faced with the challenge of combining contradicting properties that quantum technologies entail, as for example good accessibility of qubits with maximum shielding from environmental influences. In this regard, so-called two-dimensional materials, which only consist of a single layer of atoms, are particularly promising.

The team succeeded in identifying promising quantum bits in these materials. They were able to show that the qubits can be generated, read out and coherently controlled in a very robust manner.

As a matter of fact, a plethora of single-photon emitters have been identified in the atomic layers of two-dimensional van der Waals materials. The team has reported on a set of isolated optical emitters

embedded in hexagonal boron nitride that exhibit optically detected magnetic resonance. The defect spins showed an isotropic ge-factor of ∼2 and zero-field splitting below 10 MHz. The photokinetics of one type of defect is compatible with ground-state electron-spin paramagnetism. The narrow and inhomogeneously broadened magnetic resonance spectrum differs significantly from the known spectra of in-plane defects.

They determined a hyperfine coupling of ∼10 MHz. Its angular dependence indicates an unpaired, out-of-plane delocalized π-orbital electron, probably originating from substitutional impurity atoms. They extracted spin-lattice relaxation times T1 of 13-17 µs with estimated spin coherence times T2 of less than 1 µs.

These results provide further insight into the structure, composition and dynamics of single optically active spin defects in hexagonal boron nitride.

06 May 2021

41 Collaboration has mission to build UK's first commercial quantum computer

by Oxford Instruments NanoScience

https://physicsworld.com/a/collaboration-builds-uks-first-commercial-quantum-computer/

The mission to build the UK's first commercial quantum computer is gathering pace in Abingdon, Oxfordshire, at the facility of Oxford Instruments NanoScience. The UK-based manufacturer of specialist scientific equipment, including the state-of-the-art dilution refrigerators needed to operate quantum systems and other condensed-matter experiments at ultralow temperatures, is part of a consortium that is seeking to deliver a quantum computer that will start running the first end-user applications by the beginning of 2022.

The consortium, backed by a £10m investment that includes funding from the UK government's Quantum Technologies Challenge, is headed by Rigetti Computing. Headquartered in Berkeley, California, Rigetti has built a series of quantum processors based on superconducting quantum circuits that customers can program via a cloud-based platform. The latest version – the Aspen-9, which was first deployed in February – incorporates 32 qubits, and in this project the company aims to scale up the design still further.

"The system we will build here will be larger than anything we currently have available in the US," says Anna Stockklauser, Rigetti's technical lead for quantum engineering. "An initial version of the machine will be available for our UK partners to use early next year, and we will then iterate the design over time. We want to make sure that each part of the machine has been carefully proven before we build a new part of it."

As well as hosting the hardware installation, Oxford Instruments is responsible for delivering and installing the latest version of its Proteox family of dilution refrigerators, the ProteoxLX, which has been designed to provide the capacity and cooling power needed to operate large-scale quantum computers. Meanwhile, three other partners in the consortium are focused on developing quantum software and applications. The University of Edinburgh is developing new ways to test quantum hardware and the performance of quantum algorithms, and is also working with Standard Chartered Bank to advance quantum-based machine learning applications for the finance sector. The fifth partner, start-up company

Phasecraft, is using its expertise in quantum software to develop near-term applications in materials design, energy and pharmaceuticals.

The three application-focused partners are already producing results using Rigetti's US-based installations, and will switch to the UK machine as soon as it goes online. "Rigetti will be the first US quantum company to put a commercial quantum computer here in the UK, and it's amazing for us to be part of the project," says Harriet van der Vliet, product segment manager for quantum technologies at Oxford Instruments NanoScience. "It is particularly exciting to be hosting the build here at our facility, and to know that customers will be accessing the installation via the cloud."

For Rigetti, establishing a physical presence in the UK offers improved access both to local talent and expertise, and to customers – such as those in financial and government institutions – who for legal and security reasons need to keep their data within the UK. "This is a wonderful opportunity for us to get connected to the vibrant and growing quantum ecosystem in the UK," says Stockklauser. "It gives us lots of valuable links to great talent and infrastructure, as well as end users located in the UK that we hope will be able to use our machines for new purposes. It's really good to be a part of the UK's quantum sector while it is still in the making."

Stockklauser is also excited to be working with Oxford Instruments for the first time. "Oxford Instruments is one of very few companies who can build machines that are suitable for running superconducting quantum computers," she continues. "For this programme we knew we would have to do a lot of custom design work to integrate our system into the dilution refrigerator, and Oxford Instruments is a great partner for developing these custom pieces."

Quantum advantage

The ProteoxLX that Rigetti will be using to build its quantum computer is a new model in Oxford Instruments' product range, formally released just before the March Meeting of the American Physical Society in March 2021, which has been specifically designed to support quantum scale-up. It offers a significantly larger dilution unit and sample space than the original ProteoxMX, as well as more cooling power at its base temperature – which extends as low as 7 mK. "The mixing chamber plate as the sample stage of the LX has a diameter of 530 mm, compared with 360 mm for the MX," explains van der Vliet. "It also has two pulse tubes to provide more cooling power at the 4 K stage, which is useful for quantum applications that require large numbers of amplifiers."

An even more significant advantage for building large-scale quantum computers is the extra capacity the LX provides for installing quantum experiments. All the dilution refrigerators in the Proteox family are equipped with a side-loading "secondary insert" that enables an entire experimental set-up – including samples, communications wiring and signal-conditioning components – to be configured outside the refrigerator and then installed and changed whenever necessary. This modular approach allows experiments to be turned around more quickly, particularly in a multi-user environment, or where a research team might want to test different versions of a quantum chip.

What's more, the secondary inserts can be fully customized to meet the needs of the installation. "Researchers who need a number of signal-conditioning components, such as amplifiers, circulators and isolators, often want to configure their wiring in a specific way for their experiments," explains van der Vliet. "With our customizable solution we share the design drawings of the insert and work with our customers to configure the components exactly how they want them."

he LX goes one step further by incorporating two of these secondary inserts into the design, rather than

one. This essentially doubles the experimental space, offering a combination of flexibility and scalability that has proved to be a winner with Rigetti. “We need a system of the size of the ProteoxLX, and the cooling power it comes with, to be able to scale to systems with large numbers of qubits,” says Stockklauser. “Rigetti is a full-stack quantum computing company – we build the control electronics, the entire software stack, and the hardware that goes into the fridge – and the secondary insert technology has allowed us to work with Oxford Instruments to easily integrate our hardware in the dilution refrigerator with the required customizations.”

One key advantage of this approach is that the secondary inserts can be configured and fabricated before the system is installed, which reduces the time needed to get a quantum experiment up and running. Since the consortium started work in the autumn of 2020, the US and UK companies have been sharing design files to perfect the layout of the two secondary inserts, which has allowed Oxford Instruments to install the ProteoxLX – complete with the customized secondary insert – just six months after the project started.

In the cloud

Now the ProteoxLX has been installed and the final checks have been completed, the system has been fully handed over to Rigetti for the build phase of the project. Quantum engineers from Rigetti’s UK team, including Stockklauser, will be working at the Oxford site. “It’s a great set-up for us because we can run our lab with all of the infrastructure that’s already in place,” says Stockklauser. “Plus we have the expertise right here on site to provide any help we might need with operating the machines.”

For Oxford Instruments, meanwhile, the close collaboration with Rigetti offers a valuable entry point to the world of large-scale quantum computing. “It is great for the UK to have a quantum computer that will be used by customers via the cloud as the majority of commercial quantum computers are based in North America,” says van der Vliet. “This project will be great for quantum in the UK, and it’s fantastic for us as a UK company to be so heavily involved in the project. With the Rigetti team on site, we will continue our collaboration as we build our knowledge of the user experience and ensure that the ProteoxLX meets our evolving customer needs.”

42 Processing Quantum Signals Carried by Electrical Currents

by Julien-levallois

https://www.swissquantumhub.com/processing-quantum-signals-carried-by-electrical-currents/

A team of French and Dutch researchers present a general signal processing method for processing, analysing and representing electrical quantum currents directly at the level of individual electronic wave functions.

Quantum mechanics and the associated interference effects govern the laws of electricity of small conductors at low temperatures. It is responsible for its unusual properties such as deviations from the standard law of impedance composition. As spectacular as these effects may be, this image of electronic transport is still very close to the classical description of wave optics that had emerged from the 19th century.

Nevertheless, quantum electronics has recently entered a new era that cannot be grasped by any classical wave equation paradigm. Recently developed fast electron emitters generate quantum electrical currents carrying one to few elementary excitations per period, thereby bringing electronics closer to the paradigm

of quantum optics, which aims at manipulating single to few photon states of the quantum electromagnetic field. In electron quantum optics, several tomography protocols have recently been demonstrated, probing the single-particle content of time-dependent quantum electrical currents. These breakthroughs offer new possibilities such as encoding classical or quantum information with electrons, engineering quantum circuits to simulate complex many-body problems and probing them with single to few particle excitations, or developing electronic sensors, exploiting the extreme sensitivity of quantum electrical currents to the electromagnetic field. However, despite rapid progress, this field still lacks a toolbox for processing, analyzing, and representing the quantum information embedded in quantum electrical currents.

In this paper, authors present a general algorithm for extracting the single-particle wave functions present within a time-periodic quantum electrical current, their emission probabilities, and mutual coherence and apply it to the analysis of several electron sources. This work establishes the grounds for the development of signal processing of quantum electrical currents, directly at the level of electronic wave functions, a key step in the development of electron-based quantum technologies.

43 Quantum computing could be useful faster than anyone expected

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/quantum-computers-could-be-doing-useful-work-more-quickly-than-everyone-thought/

For most scientists, a quantum computer that can solve large-scale business problems is still a prospect that belongs to the distant future, and one that won't be realized for at least another decade.

But now researchers from US banking giant Goldman Sachs and quantum computing company QC Ware have designed new quantum algorithms that they say could significantly boost the efficiency of some critical financial operations – on hardware that might be available in only five years' time.

Rather than waiting for a fully-fledged quantum computer, bankers could start running the new algorithms on near-term quantum hardware and reap the benefits of the technology even while quantum devices remain immature.

Goldman Sachs has, for many years, been digging into the potential that quantum technologies have to disrupt the financial sector.

In particular, the bank's researchers have explored ways to use quantum computing to optimize what is known as Monte Carlo simulations, which consist of pricing financial assets based on how the price of other related assets change over time, and therefore accounting for the risk that is inherent to different options, stocks, currencies and commodities.

Because of the vast spectrum of possibilities, this is one of the most compute-intensive tasks in finance, which requires making large numbers of predictions about different market movements.

Quantum computing has long been identified as a potential avenue to speed up those risk assessments thanks to the extraordinary compute power that the technology is expected to bring about in comparison to classical approaches.

And many quantum algorithms exist already, which have been shown to increase the speed of Monte Carlo calculations by up to 1,000 times and could transform the way that financial markets operate – but only once those algorithms are deployed on to a quantum device that is capable of running the program, and of achieving accurate results.

Previous work carried out by Goldman Sachs together with IBM, for instance, estimated that to achieve quantum advantage would require a device supporting 7,500 logical qubits. To compare, IBM is currently working on releasing a 127-qubit processor this year.

It's not only a matter of counting qubits: for quantum computers to resolve calculations reliably, the devices will also have to be optimized to avoid errors. Current quantum processors have very high error rates, and according to QC Ware, it will be 10 to 20 years before the error-corrected quantum hardware that is necessary to efficiently run Monte Carlo simulations becomes available.

"How can we cut the current timeline in half yet still get a significant speed-up?" ask the company's researchers in a blog post describing the new research.

To achieve this objective, the team traded off some calculation speed in return for some hardware gains.

The scientists designed two new quantum algorithms that slash the speed up from 1,000 times to 100 times – but they also require a shallower circuit size, which is expected to be available in the next five to 10 years.

"The Goldman Sachs and QC Ware research teams took a novel approach to designing quantum Monte Carlo algorithms by trading off performance speed-up for reduced error rates," said Iordanis Kerenidis, head of algorithms at QC Ware.

"Through rigorous analysis and empirical simulations, we demonstrated that our Shallow Monte Carlo algorithms could result in the ability to perform Monte Carlo simulations on quantum hardware that may be available in 5 to 10 years."

The speedup, although more moderate than that of other quantum algorithms such as the QFT-free Monte Carlo, is still significant; and according to the scientists, the method will effectively cut the timeline to usability in half.

Goldman Sachs and QC Ware's efforts are reflective of an industry that is increasingly focusing on bringing about the benefits of quantum computing in the near term, despite the imperfections that are still holding quantum devices back.

Whether it is by tweaking algorithms, combining quantum and classical techniques, or testing and comparing different approaches to quantum computing, researchers and companies are racing to crack the methods that will make quantum computers useful in as little time as possible.

The two algorithms designed by Goldman Sachs and QC Ware, therefore, are yet another move towards the goal of finding quantum algorithms that are compatible with the noisy intermediate scale - NISQ – devices that are characteristic of current times.

05 May 2021

44 PsiQuantum and GLOBALFOUNDRIES to Build the World's First Full-scale Quantum Computer

https://globalfoundries.com/press-release/psiquantum-and-globalfoundries-build-worlds-first-full-scale-quantum-computer

PsiQuantum™, the leading quantum computing company focused on delivering a 1 million-plus qubit quantum computer, and GLOBALFOUNDRIES®, the global leader in feature-rich semiconductor

manufacturing, today announced a major breakthrough in their partnership to build the world's first full-scale commercial quantum computer. The two companies are now manufacturing the silicon photonic and electronic chips that form the foundation of the Q1 system, the first system milestone in PsiQuantum's roadmap to deliver a commercially viable quantum computer with one million qubits (the basic unit of quantum information) and beyond.

PsiQuantum and GF have now demonstrated a world-first ability to manufacture core quantum components, such as single-photon sources and single-photon detectors, with precision and in volume, using the standard manufacturing processes of GF's world-leading semiconductor fab. The companies have also installed proprietary production and manufacturing equipment in two of GF's 300mm fabs to produce thousands of Q1 silicon photonic chips at its facility in upstate New York, and state-of-the-art electronic control chips at its Fab 1 facility in Dresden, Germany.

Quantum computing is expected to deliver extraordinary advances across a multitude of industries including pharmaceutical development, materials science, renewable energy, climate mitigation, sustainable agriculture, and more. PsiQuantum's Q1 system represents breakthroughs in silicon photonics, which the company believes is the only way to scale to 1 million-plus qubits and beyond and to deliver an error-corrected, fault-tolerant, general-purpose quantum computer.

The Q1 system is the result of five years of development at PsiQuantum by the world's foremost experts in photonic quantum computing. The team made it their mission to bring the world-changing benefits of quantum computing into reality, based on two fundamental understandings:

(i) A useful quantum computer capable of performing otherwise impossible calculations requires 1 million-plus physical qubits; and

(ii) Leveraging the 50-plus years and trillions of dollars invested in the semiconductor industry is the only path to create a commercially viable quantum computer.

"In the past year, we have experienced a decade of technological change. Now, due to the digital transformation and the explosion of data we are faced with problems that require quantum computing to further accelerate the Renaissance of Compute," said Amir Faintuch, senior vice president and general manager of Compute and Wired Infrastructure at GF. "PsiQuantum and GF's partnership is a powerful combination of PsiQuantum's photonic quantum computing expertise and GF's silicon photonics manufacturing capability that will transform industries and technology applications across climate, energy, healthcare, materials science, and government."

GF's leading silicon photonics manufacturing platform enables PsiQuantum to develop quantum chips that can be measured and tested for long-term performance reliability. This is critical to be able to execute quantum algorithms, which require millions or billions of gate operations. PsiQuantum is collaborating with researchers, scientists and developers at leading companies to explore and test quantum use cases across a range of industries, including energy, healthcare, finance, agriculture, transportation and communications.

"This is a major achievement for both the quantum and semiconductor industries, demonstrating that it's possible to build the critical components of a quantum computer on a silicon chip, using the standard manufacturing processes of a world-leading semiconductor fab," said Pete Shadbolt, chief strategy officer and co-founder of PsiQuantum. "When we first envisioned PsiQuantum, we knew that scaling the system would be the existential question. Together with GLOBALFOUNDRIES, we have validated the manufacturing path for silicon photonics and are confident that by the middle of this decade, PsiQuantum

will have completely stood up all the manufacturing lines and processes necessary to begin assembling a final machine."

The PsiQuantum and GF partnership is redefining the leading-edge by enabling the move from electrons to photons, while the rest of the world continues to chase traditional node scaling. Moreover, the partnership is playing a critical role in ensuring the United States becomes a global leader in quantum computing, supported by a secure, domestic supply chain. As the only semiconductor manufacturer with a global footprint, GF provides a broad range of platforms with feature-rich solutions enabling customers to develop pervasive products for high-growth market segments.

45 Researchers confront major hurdle in quantum computing

by University of Rochester

https://phys.org/news/2021-05-major-hurdle-quantum.html

In a series of papers, Rochester researchers report major strides in improving the transfer of information in quantum systems.

Quantum science has the potential to revolutionize modern technology with more efficient computers, communication, and sensing devices. But challenges remain in achieving these technological goals, especially when it comes to effectively transferring information in quantum systems.

A regular computer consists of billions of transistors, called bits. Quantum computers, on the other hand, are based on quantum bits, also known as qubits, which can be made from a single electron.

Unlike ordinary transistors, which can be either "0" (off) or "1" (on), qubits can be both "0" and "1" at the same time. The ability of individual qubits to occupy these so-called superposition states, where they are in multiple states simultaneously, underlies the great potential of quantum computers. Just like ordinary computers, however, quantum computers need a way to transfer quantum information between distant qubits – and that presents a major experimental challenge.

In a series of papers published in Nature Communications, researchers at the University of Rochester, including John Nichol, an assistant professor of physics and astronomy, and graduate students Yadav Kandel and Haifeng Qiao, the lead authors of the papers, report major strides in enhancing quantum computing by improving the transfer of information between electrons in quantum systems.

In one paper, the researchers demonstrated a route of transferring information between qubits, called adiabatic quantum state transfer (AQT), for the first time with electron-spin qubits. Unlike most methods of transferring information between qubits, which rely on carefully tuned electric or magnetic-field pulses, AQT isn't as affected by pulse errors and noise.

To envision how AQT works, imagine you are driving your car and want to park it. If you don't hit your brakes at the proper time, the car won't be where you want it, with potential negative consequences. In this sense, the control pulses – the gas and brake pedals – to the car must be tuned carefully. AQT is different in that it doesn't really matter how long you press the pedals or how hard you press them: the car will always end up in the right spot. As a result, AQT has the potential to improve the transfer of information between qubits, which is essential for quantum networking and error correction.

The researchers demonstrated AQT's effectiveness by exploiting entanglement – one of the basic concepts of quantum physics in which the properties of one particle affect the properties of another, even

when the particles are separated by a large distance. The researchers were able to use AQT to transfer one electron's quantum spin state across a chain of four electrons in semiconductor quantum dots – tiny, nanoscale semiconductors with remarkable properties. This is the longest chain over which a spin state has ever been transferred, tying the record set by the researchers in a previous Nature paper.

"Because AQT is robust against pulse errors and noise, and because of its major potential applications in quantum computing, this demonstration is a key milestone for quantum computing with spin qubits," Nichol says.

Exploiting a strange state of matter

In a second paper, the researchers demonstrated another technique of transferring information between qubits, using an exotic state of matter called time crystals. A time crystal is a strange state of matter in which interactions between the particles that make up the crystal can stabilize oscillations of the system in time indefinitely. Imagine a clock that keeps ticking forever; the pendulum of the clock oscillates in time, much like the oscillating time crystal.

By implementing a series of electric-field pulses on electrons, the researchers were able to create a state similar to a time crystal. They found that they could then exploit this state to improve the transfer of an electron's spin state in a chain of semiconductor quantum dots.

"Our work takes the first steps toward showing how strange and exotic states of matter, like time crystals, can potentially by used for quantum information processing applications, such as transferring information between qubits," Nichol says. "We also theoretically show how this scenario can implement other single- and multi-qubit operations that could be used to improve the performance of quantum computers."

Both AQT and time crystals, while different, could be used simultaneously with quantum computing systems to improve performance.

"These two results illustrate the strange and interesting ways that quantum physics allows for information to be sent from one place to another, which is one of the main challenges in constructing viable quantum computers and networks," Nichol says.

04 May 2021

46 Three new malware families found in global finance phishing campaign

by Charlie Osborne

https://www.zdnet.com/article/researchers-find-three-new-malware-families-used-in-global-finance-phishing-campaign/

Researchers have found three new malware families used in a widespread phishing campaign entrenched in financial crime.

On Tuesday, FireEye's Mandiant cybersecurity team said the malware strains, dubbed Doubledrag, Doubledrop, and Doubleback, were detected in December 2020.

The threat actors behind the malware, described as "experienced and well-resourced," are being tracked as UNC2529.

Organizations in the US, EMEA region, Asia, and Australia have, so far, been targeted in two separate waves.

Phishing messages sent to potential victims were rarely based on the same email addresses and subject lines were tailored to targets; in many cases, threat actors would masquerade as account executives touting services suitable for different industries – including defense, medicine, transport, the military, and electronics.

Over 50 domains, in total, were used to manage the global phishing scheme. In one successful attack, UNC2529 successfully compromised a domain owned by a US heating and cooling services business, tampered with its DNS records, and used this structure to launch phishing attacks against at least 22 organizations.

The lure emails contained links to URLs leading to malicious .PDF payloads and an accompanying JavaScript file contained in a .zip archive. The documents, fetched from public sources, were corrupted to render them unreadable – and so it is thought that victims might become annoyed enough to double-click the .js file in an attempt to read the content.

Mandiant says the .js file, that is heavily obfuscated, contains the Doubledrag downloader. Alternatively, some campaigns have used an Excel document with an embedded macro to deliver the same payload.

Upon execution, Doubledrag attempts to download a dropper as the second stage of the attack chain. This dropper, Doubledrop, is an obfuscated PowerShell script designed to establish a foothold into an infected machine by loading a backdoor into memory.

The backdoor is the final malware component, Doubleback, malware created in both 32-bit and 64-bit versions.

"The backdoor, once it has the execution control, loads its plugins and then enters a communication loop, fetching commands from its [command-and-control] C2 server and dispatching them," Mandiant notes. "One interesting fact about the whole ecosystem is that only the downloader exists in the file system. The rest of the components are serialized in the registry database, which makes their detection somewhat harder, especially by file-based antivirus engines."

There are some indicators that the malware is still in progress, as existing functionality will scan for the existence of antivirus products – such as those offered by Kaspersky and BitDefender – but even if detected, no action is taken.

Analysis of the new malware strains is ongoing.

"Although Mandiant has no evidence about the objectives of this threat actor, their broad targeting across industries and geographies is consistent with a targeting calculus most commonly seen among financially motivated groups," the researchers say.

47 Complex shapes of photons to boost future quantum technologies

by Tampere University

https://www.sciencedaily.com/releases/2021/05/210504112529.htm#:~:text=Complex%20shapes%20of%20photons%20to%20boost%20future%20quantum%20technologies,-Date%3A%20May%204&text=Summary%3A,computations%20and%20safe%20data%20transfer.

As the digital revolution has now become mainstream, quantum computing and quantum communication are rising in the consciousness of the field. The enhanced measurement technologies enabled by quantum phenomena, and the possibility of scientific progress using new methods, are of particular interest to researchers around the world.

Recently two researchers at Tampere University, Assistant Professor Robert Fickler and Doctoral Researcher Markus Hiekkamäki, demonstrated that two-photon interference can be controlled in a near-perfect way using the spatial shape of the photon. Their findings were recently published in the journal Physical Review Letters.

"Our report shows how a complex light-shaping method can be used to make two quanta of light interfere with each other in a novel and easily tuneable way," explains Markus Hiekkamäki.

Single photons (units of light) can have highly complex shapes that are known to be beneficial for quantum technologies such as quantum cryptography, super-sensitive measurements, or quantum-enhanced computational tasks. To make use of these so-called structured photons, it is crucial to make them interfere with other photons.

"One crucial task in essentially all quantum technological applications is improving the ability to manipulate quantum states in a more complex and reliable way. In photonic quantum technologies, this task involves changing the properties of a single photon as well as interfering multiple photons with each other;" says Robert Fickler, who leads the Experimental Quantum Optics group at the university.

Linear optics bring promising solutions to quantum communications

The demonstrated development is especially interesting from the point of view of high-dimensional quantum information science, where more than a single bit of quantum information is used per carrier. These more complex quantum states not only allow the encoding of more information onto a single photon but are also known to be more noise-resistant in various settings.

The method presented by the research duo holds promise for building new types of linear optical networks. This paves the way for novel schemes of photonic quantum-enhanced computing.

"Our experimental demonstration of bunching two photons into multiple complex spatial shapes is a crucial next step for applying structured photons to various quantum metrological and informational tasks," continues Markus Hiekkamäki.

The researchers now aim at utilizing the method for developing new quantum-enhanced sensing techniques, while exploring more complex spatial structures of photons and developing new approaches for computational systems using quantum states.

"We hope that these results inspire more research into the fundamental limits of photon shaping. Our findings might also trigger the development of new quantum technologies, e.g. improved noise-tolerant quantum communication or innovative quantum computation schemes, that benefit from such high-dimensional photonic quantum states," adds Robert Fickler.

03 May 2021

48 NIST previews post-quantum cryptography challenges

by susan miller

https://gcn.com/articles/2021/05/03/nist-post-quantum-encryption.aspx

To help prepare organizations for post-quantum cryptography, the National Institute of Standards and Technology's National Cybersecurity Center of Excellence has released the final version of a white paper, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms."

Since 2016, NIST has been working with researchers to develop cryptographic algorithms that will be strong enough to resist the privacy and security threats quantum computers will pose. While those new algorithms will likely be ready before quantum computers are widely used, the transition from today's standards to the new post-quantum public-key standards "is likely to be more problematic than the introduction of new classical cryptographic algorithms," the paper states. "In the absence of significant implementation planning, it may be decades before the community replaces most of the vulnerable public-key systems currently in use."

One problem is that existing encryption standards can't simply be replaced with quantum-resistant ones. Some quantum-resistant candidate algorithms involve extremely large signature sizes, require excessive processing and use very large public or private keys that would make the solution difficult to implement widely. Even when secure operations are possible, NIST says, "performance and scalability issues may demand significant modifications to protocols and infrastructures."

As a result, there might need to be a variety of post-quantum algorithms to overcome implementation constraints, like sensitivity to large signature sizes. Another option would require modifying existing protocols to handle larger signatures. In any case, the report says, replacing cryptographic algorithms will be a large and complex operation that requires "changing or replacing cryptographic libraries, implementation validation tools, hardware that implements or accelerates algorithm performance, dependent operating system and application code, communications devices and protocols, and user and administrative procedures."

Consequently, detailed migration roadmaps and playbooks must be developed to help organizations first discover where and how public-key cryptography is currently being used and then determine where migration to post-quantum cryptography will be required. In some cases, migration from classical to post-quantum encryption may involve temporarily depending on hybrid algorithms. If requirements for some use cases can be defined early enough, they can be fed into the standards development process.

"We need to determine where, why, and with what priority vulnerable public-key algorithms will need to be replaced, and we need to understand the constraints that apply to specific use cases," NIST states. "These initial steps in developing and implementing algorithm migration playbooks can and should begin immediately."

49 Beyond Qubits: Key Components for a Qutrit-Based Quantum Computer Demonstrated

by lawrence berkeley national laboratory

https://scitechdaily.com/beyond-qubits-key-components-for-a-qutrit-based-quantum-computer-demonstrated/

A team led by physicists at Lawrence Berkeley National Laboratory (Berkeley Lab) and UC Berkeley has successfully observed the scrambling of quantum information, which is thought to underlie the behavior of

black holes, using qutrits: information-storing quantum units that can represent three separate states at the same time. Their efforts also pave the way for building a quantum information processor based upon qutrits.

The black hole information paradox

The new study, recently published in the journal Physical Review X, makes use of a quantum circuit that is inspired by the longstanding physics question: What happens to information when it enters a black hole?

Beyond the connection to cosmology and fundamental physics, the team's technical milestones that made the experiment possible represent important progress toward using more complex quantum processors for quantum computing, cryptography, and error detection, among other applications.

While black holes are considered one of the most destructive forces in the universe – matter and light cannot escape their pull, and are quickly and thoroughly scrambled once they enter – there has been considerable debate about whether and how information is lost after passing into a black hole.

The late physicist Stephen Hawking showed that black holes emit radiation – now known as Hawking radiation – as they slowly evaporate over time. In principle, this radiation could carry information about what's inside the black hole – even allowing the reconstruction of information that passes into the black hole.

And by using a quantum property known as entanglement, it is possible to perform this reconstruction significantly more rapidly, as was shown in earlier work.

Quantum entanglement defies the rules of classical physics, allowing particles to remain correlated even when separated by large distances so that the state of one particle will inform you about the state of its entangled partner. If you had two entangled coins, for example, knowing that one coin came up heads when you looked at it would automatically tell you that the other entangled coin was tails, for example.

Most efforts in quantum computing seek to tap into this phenomenon by encoding information as entangled quantum bits, known as qubits (pronounced CUE-bits). Like a traditional computer bit, which can hold the value of zero or one, a qubit can also be either a zero or one. But in addition, a qubit can exist in a superposition that is both one and zero at the same time. In the case of a coin, it's like a coin flip that can represent either heads or tails, as well as the superposition of both heads and tails at the same time.

The power of 3: Introducing qutrits

Each qubit you add to a quantum computer doubles its computing power, and that exponential increase soars when you use quantum bits capable of storing more values, like qutrits. Because of this, it takes far fewer qubits and even fewer qutrits or qudits – which describes quantum units with three or more states – to perform complex algorithms capable of demonstrating the ability to solve problems that cannot be solved using conventional computers.

That said, there are a number of technical hurdles to building quantum computers with a large number of quantum bits that can operate reliably and efficiently in solving problems in a truly quantum way.

In this latest study, researchers detail how they developed a quantum processor capable of encoding and transmitting information using a series of five qutrits, which can each simultaneously represent three

states. And despite the typically noisy, imperfect, and error-prone environment of quantum circuity, they found that their platform proved surprisingly resilient and robust.

Qutrits can have a value of zero, one, or two, holding all of these states in superposition. In the coin analogy, it's like a coin that has the possibility of coming up as heads, tails, or in landing on its thin edge.

"A black hole is an extremely good encoder of information," said Norman Yao, a faculty scientist in Berkeley Lab's Materials Sciences Division and an assistant professor of physics at UC Berkeley who helped to lead the planning and design of the experiment. "It smears it out very quickly, so that any local noise has an extremely hard time destroying this information."

But, he added, "The encoder is so darn good that it's also very hard to decode this information."

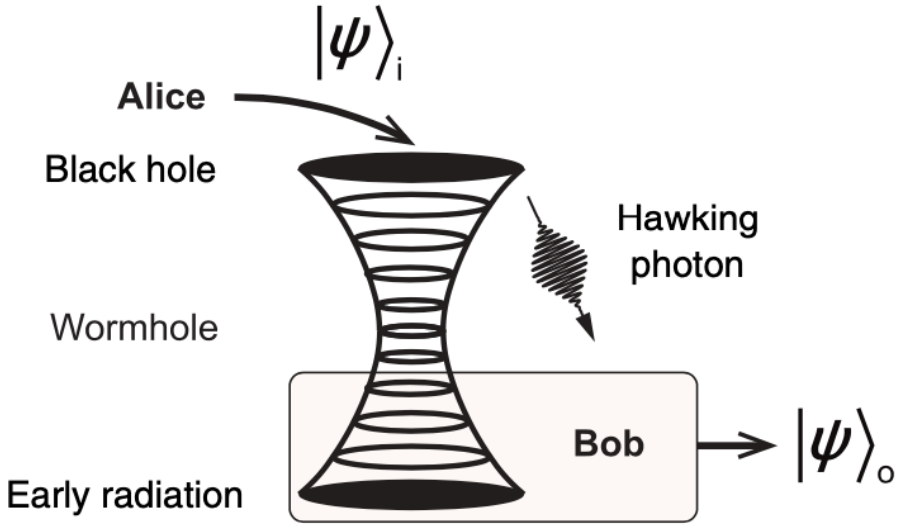


Figure 1: An illustration of a thought experiment in which information dropped into a black hole by Alice is recovered by an outside observer Bob.

Creating an experiment to mimic quantum scrambling

The team set out to replicate the type of rapid quantum information smearing, or scrambling, in an experiment that used tiny devices called nonlinear harmonic oscillators as qutrits. These nonlinear harmonic oscillators are essentially sub-micron-sized weights on springs that can be driven at several distinct frequencies when subjected to microwave pulses.

A common problem in making these oscillators work as qutrits, though, is that their quantum nature tends to break down very quickly via a mechanism called decoherence, so it is difficult to distinguish whether the information scrambling is truly quantum or is due to this decoherence or other interference, noted Irfan Siddiqi, the study's lead author.

Siddiqi is director of Berkeley Lab's Advanced Quantum Testbed, a faculty scientist in the Lab's Computational Research and Materials Sciences divisions, and a professor of physics at UC Berkeley.

The testbed, which began accepting proposals from the quantum science community in 2020, is a collaborative research laboratory that provides open, free access to users who want to explore how superconducting quantum processors can be used to advance scientific research. The demonstration of scrambling is one of the first results from the testbed's user program.

"In principle, an isolated black hole exhibits scrambling," Siddiqi said, "but any experimental system also exhibits loss from decoherence. In a laboratory, how do you distinguish between the two?"

A key to the study was in preserving the coherence, or orderly patterning, of the signal carried by the oscillators for long enough to confirm that quantum scrambling was occurring via the teleportation of a qutrit. While teleportation may conjure up sci-fi imagery of "beaming up" people or objects from a planet's surface onto a spaceship, in this case there is only the transmission of information – not matter – from one location to another via quantum entanglement.

Another essential piece was the creation of customized logic gates that enable the realization of "universal quantum circuits," which can be used to run arbitrary algorithms. These logic gates allow pairs of qutrits to interact with each other and were designed to handle three different levels of signals produced by the microwave pulses.

One of the five qutrits in the experiment served as the input, and the other four qutrits were in entangled pairs. Because of the nature of the qutrits' entanglement, a joint measurement of one of the pairs of qutrits after the scrambling circuit ensured that the state of the input qutrit was teleported to another qutrit.

Mirrored black holes and wormholes

The researchers used a technique known as quantum process tomography to verify that the logic gates were working and that the information was properly scrambled, so that it was equally likely to appear in any given part of the quantum circuit.

Siddiqi said that one way to think about how the entangled qutrits transmit information is to compare it to a black hole. It's as if there is a black hole and a mirrored version of that black hole, so that information passing in one side of the mirrored black hole is transmitted to the other side via entanglement.

Looking forward, Siddiqi and Yao are particularly interested in tapping into the power of qutrits for studies related to traversable wormholes, which are theoretical passages connecting separate locations in the universe, for example.

50 A buyer's guide to quantum as a service: Qubits for hire

by Scott Fulton III

https://www.zdnet.com/article/a-buyers-guide-to-quantum-as-a-service-qubits-for-hire/

Steve Jobs is widely quoted to have said, "A lot of times, people don't know what they want until you show it to them." A quantum computing (QC) service is hard enough to understand when it's explained to you plainly. The promise of QC relies upon its ability to leverage something weird to accomplish something fantastic. Thing is, we're not quite at "fantastic" yet, and by the time we get there, things may no longer be so weird.

Here's the general idea: The first quantum computing (QC) services, or quantum-like services, being offered to commercial customers are experiments. They are ways to stage scientific functions, in an effort to learn where a quantum-oriented market might be. That's important because QC researchers need to be able to tap into this market as early as possible (assuming it exists) if they are to generate the capital investments necessary to actually grow such a market in the first place.

To give you a better sense of where this market stands at the moment, we've selected five organizations – some commercial, some academic, and some which blend the two – which offer some kind of a quantum computing service that incorporates real QCs performing true quantum functions. The expectation is that customers will be able to subscribe to quantum services much the same way they do to cloud services today, whether that's a first or at some eventual point in time. The thing with quantum is, time ends up more often than not being a variable.

Why we chose these five

As we are not quantum researchers, and as the present state of the market is perhaps just one stage beyond embryonic, we're frankly not in a position to make recommendations based on overall, long-term quality of service. What we do know about, from experience, is the development of technology and software markets – particularly how certain players position themselves to be, or to eventually become, influential.

So we chose five QaaS services that show signs of being influential and becoming the models for others as this market develops. These are services that, based partly upon who provides them but also upon the cleverness of their value propositions, we believe will shape the course of this emerging industry ... assuming, of course, it continues to emerge.

- **Amazon Braket**

  Braket seems the most fitting prototype for the type of quantum computing service that could become commonplace, should QC essentially work the way we predict it should at present. It presumes its customer is a developer, and that this customer's objective is to use development tools to devise a quantum circuit, which is a simulated device whose schematics follow the principles of quantum physics as we understand them.

  At a very deep level, all computer programs may be decompiled into a fundamental form called a Boolean circuit, whose logic may be depicted on a flowchart. A quantum circuit has a graphic form as well, and as with classical, binary computers, there are languages and symbologies that make it easier for a developer to express the logic of such a circuit. For instance, there's the so-called "Bra-Ket" notation that uses characters such as $|v\rangle$ and $\langle v|$ to represent vectorization and linearization, respectively, when mapping the state of one quantum system to another, created by quantum physics pioneer Paul Dirac in 1934, and for which AWS' system is named.

  Suppose the broader application you're writing calls upon you to take a very complex audio waveform, and decompose it into a series of constituent, simpler waves that can be described in terms of frequency and amplitude. A classical Fourier transform algorithm can accomplish this, only with recursion – it needs several iterations before arriving at a result. With a properly constructed quantum circuit, such a transform can be accomplished with just one pass.

  Braket starts by giving you the tools you'd need to build the quantum circuit linguistically, and then test that circuit ("printing" it) against AWS' online quantum simulator – an application running on the Amazon cloud, which garners $0.075 or $0.275 per active minute (first hour free), depending on service grade – or the local simulator, which is an application you can run locally on your PC. Such a simulator doesn't quite provide a full solution, though it may reveal enough data to tell you whether the circuit is error-free. Note you don't have to spin up your own AWS virtual machine; the staging area provides just the resources you need to "print" the circuit.

  After that point, AWS serves as a kind of broker for a handful of other providers' real (not simulated) quantum computers. Through an online marketplace that should look familiar enough to regular AWS

users, Bracket facilitates transactions that let you stage your tested circuit on one of these real QCs. You settle the price with your choice of QPU provider, at a base price of $0.30 per task, plus a surplus fee per "shot" (a very generalized way of symbolizing a program cycle). Using an open source software development kit (SDK) called Qiskit, you can then make your quantum circuit accessible by a classical application.

- **QuTech Quantum Inspire**

  Quantum Inspire is an ongoing project by the Netherlands' Delft University of Technology (TU Delft), collaborating with the Dutch research organization TNO, to prototype a network of QC systems that can be put to use for commercial and academic purposes. In a March 2020 white paper introducing the platform, TU Delft's researchers explained that the intention of their system is to model not just the QC, but the entire computing economy that will make QaaS available and useful at some point:

  > Quantum Inspire comprises of a number of layers including quantum hardware, classical control electronics, and a software front-end with a cloud-accessible web-interface. Such a system is called a full-stack. Full-stack systems are essential test beds for understanding this novel computational paradigm. They can act as technology accelerators because only through careful analysis of the individual system layers and their interdependencies is it possible to detect the gaps and necessary next steps in the innovation roadmap and supply chain.

  At the time of this writing, in addition to a pair of simulators, Quantum Inspire utilized two genuine QPU-based backends:

  - **Spin-2**, comprised of a two-qubit quantum dot suspended in purified Silicon 28, designed more as an experiment in creating quantum processors using more conventional lithographic techniques;
  - **Starmon-5**, comprised of five qubits in a X-formation, testing the resonant characteristics of qubits in close proximity to one another.

  For this project, TU Delft developed its own quantum assembly language, entitled cQASM. It specifies a sequence of logical operations, more like a notation than a language. When a programmer specifies a quantum circuit using cQASM, the Quantum Inspire editor generates a graph of the circuit, like the simple one above. There, an "H" box represents a two-qubit logic gate, called a Hadamard gate. It's one of the visual tools used to generate an expression of a quantum circuit – in quantum terms, to generate a Hamiltonian.

- **D-Wave Leap / Leap2**

  There continues to be considerable debate in academic circles as to whether quantum annealing qualifies as quantum computing, since its ultimate objective is not so much to solve problems as to optimize or refine problem solving. While that debate goes on, one of the earliest organizations to offer any kind of functional quantum product, D-Wave Systems, offers cloud-based access to its annealing systems, by way of Leap (whose premium service tier is called Leap2).

  Although annealing is only suited to modeling certain classes of problems, it's arguably well-suited. Rather than modeling an algorithm as a kind of circuit, as with conventional QC, annealing adopts a probabilistic model. In one sense, this model resembles the weights and biases applied to a neural network.

The trick for the developer is being able to rephrase the mathematical function in question in the form of an "energy model." Since qubits in quantum superposition (in-between 0 and 1) tend to seek a low-energy state, an energy model can leverage this fact of physics by building a kind of subatomic Plinko machine for solutions to fall into. Here, more probable results dig deeper pits for qubits to fall into, while less probable ones leave shallower pits. If you can accept the results of your operation as probabilities rather than facts, this method could yield more reliable probabilistic estimates. It's actually the same leap of faith, if you will, that researchers in neural computing science have made, and their investments have paid off handsomely.

So what really are Leap and Leap2 for? If you're a statistical researcher or mathematician, and you believe that algorithms are the most reliable ways to attain reliable probability measures, then there's a very good argument that annealing can yield the most reliable estimates possible of uncertainty levels. There's little plus-or-minus factor; you know how uncertain you are, and that can be a benefit.

- **Honeywell H0 /H1**

  Until there is an official scorekeeper for this industry, Honeywell Quantum Solutions may have to be taken at its word that its trapped-ion qubit fabrication method enables up to 64 qubits to become entangled. Think of each qubit as a memory component. The number of possible superposition states for each entangled qubit (analogous to the length of a byte in binary computing) grows to 2, raised to the power of the number of qubits. So 64 is a much bigger stretch from 63 than 63 was from 62.

  Honeywell's primary interest in QC is to eventually sell commercial hardware, but in the meantime, sell commercial quantum services. Up until recently, its primary means of building a customer base had been direct collaboration – getting academia involved in the design process. In October 2020, the company took its outreach program one step further, by selling time on one of its H0 or H1 models, for a presumably nominal fee. It's very transparent about its motives: It's seeking greater involvement by potential customers, as a way of inspiring its own engineers to make process improvements for its forthcoming H2 model.

  So this isn't exactly a serve-yourself, self-provisioning, cloud-like service: With Honeywell, the idea is that you're entering into a professional, customer relationship with the manufacturer, perhaps with the idea of giving its machines a test-drive.

- **Strangeworks Quantumcomputing.com**

  Essentially, Strangeworks has built a collaboration platform for quantum researchers, encouraging them to come together and share their work with each other – and the emerging community – under an open source license. The platform was launched with a QC simulator only, though its executives have plans to facilitate direct access to a working QC facility. In the meantime, the platform serves as a marketplace where participants may serve as vendors.

  The effort stemmed from founder William "Whurley" Hurley's work as chair of the IEEE's Quantum Computing Working Group. As his day job, Hurley built applications platforms either for, or to be acquired by, major enterprises. For instance, in 2014, Hurley built an investment advice expert system called Honest Dollar, which was acquired two years later by investment firm Goldman Sachs. Experiences such as this informed Hurley that scientific computing entrepreneurs need exposure to investment capital first and foremost. His objective for Strangeworks has been to bring together the class of people he's worked with at IEEE, and make their services and expertise accessible to potential benefactors, thus germinating the kind of ecosystem that QC has yet to attain under its own power.

51 World's 1st multinode quantum network is a breakthrough for the quantum internet

by Ben Turner

https://www.livescience.com/three-node-quantum-network.html

Scientists have gotten one step closer to a quantum internet by creating the world's first multinode quantum network.

Researchers at the QuTech research center in the Netherlands created the system, which is made up of three quantum nodes entangled by the spooky laws of quantum mechanics that govern subatomic particles. It is the first time that more than two quantum bits, or "qubits," that do the calculations in quantum computing have been linked together as "nodes," or network endpoints.

Researchers expect the first quantum networks to unlock a wealth of computing applications that can't be performed by existing classical devices – such as faster computation and improved cryptography.

"It will allow us to connect quantum computers for more computing power, create unhackable networks and connect atomic clocks and telescopes together with unprecedented levels of coordination," Matteo Pompili, a member of the QuTech research team that created the network at Delft University of Technology in the Netherlands, told Live Science. "There are also loads of applications that we can't really foresee. One could be to create an algorithm that will run elections in a secure way, for instance."

In much the same way that the traditional computer bit is the basic unit of digital information, the qubit is the basic unit of quantum information. Like the bit, the qubit can be either a 1 or a 0, which represent two possible positions in a two-state system.

But that's just about where the similarities end. Thanks to the bizarre laws of the quantum world, the qubit can exist in a superposition of both the 1 and 0 states until the moment it is measured, when it will randomly collapse into either a 1 or a 0. This strange behavior is the key to the power of quantum computing, as it allows a qubit to perform multiple calculations simultaneously.

The biggest challenge in linking those qubits together into a quantum network is in establishing and maintaining a process called entanglement, or what Albert Einstein dubbed "spooky action at a distance." This is when two qubits become coupled, linking their properties so that any change in one particle will cause a change in the other, even if they are separated by vast distances.

You can entangle quantum nodes in a lot of ways, but one common method works by first entangling the stationary qubits (which form the network's nodes) with photons, or light particles, before firing the photons at each other. When they meet, the two photons also become entangled, thereby entangling the qubits. This binds the two stationary nodes that are separated by a distance. Any change made to one is reflected by an instantaneous change to the other.

"Spooky action at a distance" lets scientists change the state of a particle by altering the state of its distant entangled partner, effectively teleporting information across big gaps. But maintaining a state of entanglement is a tough task, especially as the entangled system is always at risk of interacting with the outside world and being destroyed by a process called decoherence.

This means, first, that the quantum nodes have to be kept at extremely cold temperatures inside devices called cryostats to minimize the chances that the qubits will interfere with something outside the system. Second, the photons used in the entanglement can't travel very long distances before they are absorbed or

scattered, – destroying the signal being sent between two nodes.

"The problem is, unlike classical networks, you cannot amplify quantum signals. If you try to copy the qubit, you destroy the original copy," Pompili said, referring to physics' "no-cloning theorem," which states that it is impossible to create an identical copy of an unknown quantum state. "This really limits the distances we can send quantum signals to the tens of hundreds of kilometers. If you want to set up quantum communication with someone on the other side of the world, you'll need relay nodes in between."

To solve the problem, the team created a network with three nodes, in which photons essentially "pass" the entanglement from a qubit at one of the outer nodes to one at the middle node. The middle node has two qubits – one to acquire an entangled state and one to store it. Once the entanglement between one outer node and the middle node is stored, the middle node entangles the other outer node with its spare qubit. With all of this done, the middle node entangles its two qubits, causing the qubits of the outer nodes to become entangled.

But designing this weird quantum mechanical spin on the classic "river crossing puzzle" was the least of the researchers' troubles – weird, for sure, but not too tricky an idea. To make the entangled photons and beam them to the nodes in the right way, the researchers had to use a complex system of mirrors and laser light. The really tough part was the technological challenge of reducing pesky noise in the system, as well as making sure all of the lasers used to produce the photons were perfectly synchronized.

"We're talking about having three to four lasers for every node, so you start to have 10 lasers and three cryostats that all need to work at the same time, along with all of the electronics and the synchronization," Pompili said.

The three-node system is particularly useful as the memory qubit allows researchers to establish entanglement across the network node by node, rather than the more demanding requirement of doing it all at once. As soon as this is done, information can be beamed across the network.

Some of the researchers' next steps with their new network will be to attempt this information beaming, along with improving essential components of the network's computing abilities so that they can work like regular computer networks do. All of these things will set the scale that the new quantum network could reach.

They also want to see if their system will allow them to establish entanglement between Delft and The Hague, two Dutch cities that are roughly 6 miles (10 kilometers) apart.

"Right now, all of our nodes are within 10 to 20 meters [32 to 66 feet] of each other," Pompili said. "If you want something useful, you need to go to kilometers. This is going to be the first time that we're going to make a link between long distances."

01 May 2021

52 Scientists discover new vulnerability affecting computers globally

by Audra Book

https://techxplore.com/news/2021-04-scientists-vulnerability-affecting-globally.amp

In 2018, industry and academic researchers revealed a potentially devastating hardware flaw that made computers and other devices worldwide vulnerable to attack.

Researchers named the vulnerability Spectre because the flaw was built into modern computer processors that get their speed from a technique called "*speculative execution*," in which the processor predicts instructions it might end up executing and preps by following the predicted path to pull the instructions from memory. A Spectre attack tricks the processor into executing instructions along the wrong path. Even though the processor recovers and correctly completes its task, hackers can access confidential data while the processor is heading the wrong way.

Since Spectre was discovered, the world's most talented computer scientists from industry and academia have worked on software patches and hardware defenses, confident they've been able to protect the most vulnerable points in the speculative execution process without slowing down computing speeds too much.

They will have to go back to the drawing board.

A team of University of Virginia School of Engineering computer science researchers has uncovered a line of attack that breaks all Spectre defenses, meaning that billions of computers and other devices across the globe are just as vulnerable today as they were when Spectre was first announced. The team reported its discovery to international chip makers in April and will present the new challenge at a worldwide computing architecture conference in June.

The researchers, led by Ashish Venkat, William Wulf Career Enhancement Assistant Professor of Computer Science at UVA Engineering, found a whole new way for hackers to exploit something called a "micro-op cache," which speeds up computing by storing simple commands and allowing the processor to fetch them quickly and early in the speculative execution process. Micro-op caches have been built into Intel computers manufactured since 2011.

Venkat's team discovered that hackers can steal data when a processor fetches commands from the micro-op cache.

"Think about a hypothetical airport security scenario where TSA lets you in without checking your boarding pass because

(i) it is fast and efficient, and

(ii) you will be checked for your boarding pass at the gate anyway," Venkat said.

"A computer processor does something similar. It predicts that the check will pass and could let instructions into the pipeline. Ultimately, if the prediction is incorrect, it will throw those instructions out of the pipeline, but this might be too late because those instructions could leave side-effects while waiting in the pipeline that an attacker could later exploit to infer secrets such as a password."

Because all current Spectre defenses protect the processor in a later stage of speculative execution, they are useless in the face of Venkat's team's new attacks. Two variants of the attacks the team discovered can steal speculatively accessed information from Intel and AMD processors.

"Intel's suggested defense against Spectre, which is called LFENCE, places sensitive code in a waiting area until the security checks are executed, and only then is the sensitive code allowed to execute," Venkat said. "But it turns out the walls of this waiting area have ears, which our attack exploits. We show how an attacker can smuggle secrets through the micro-op cache by using it as a covert channel."

Venkat's team includes three of his computer science graduate students, Ph.D. student Xida Ren, Ph.D. student Logan Moody and master's degree recipient Matthew Jordan. The UVA team collaborated with Dean Tullsen, professor of the Department of Computer Science and Engineering at the University

of California, San Diego, and his Ph.D. student Mohammadkazem Taram to reverse-engineer certain undocumented features in Intel and AMD processors.

They have detailed the findings in their paper: "I See Dead µops: Leaking Secrets via Intel/AMD Micro-Op Caches."

This newly discovered vulnerability will be much harder to fix.

"In the case of the previous Spectre attacks, developers have come up with a relatively easy way to prevent any sort of attack without a major performance penalty" for computing, Moody said. "The difference with this attack is you take a much greater performance penalty than those previous attacks."

"Patches that disable the micro-op cache or halt speculative execution on legacy hardware would effectively roll back critical performance innovations in most modern Intel and AMD processors, and this just isn't feasible," Ren, the lead student author, said.

"It is really unclear how to solve this problem in a way that offers high performance to legacy hardware, but we have to make it work," Venkat said. "Securing the micro-op cache is an interesting line of research and one that we are considering."

Venkat's team has disclosed the vulnerability to the product security teams at Intel and AMD. Ren and Moody gave a tech talk at Intel Labs worldwide April 27 to discuss the impact and potential fixes. Venkat expects computer scientists in academia and industry to work quickly together, as they did with Spectre, to find solutions.

The team's paper has been accepted by the highly competitive International Symposium on Computer Architecture, or ISCA. The annual ISCA conference is the leading forum for new ideas and research results in computer architecture and will be held virtually in June.

Venkat is also working in close collaboration with the Processor Architecture Team at Intel Labs on other microarchitectural innovations, through the National Science Foundation/Intel Partnership on Foundational Microarchitecture Research Program.

Venkat was well prepared to lead the UVA research team into this discovery. He has forged a long-running partnership with Intel that started in 2012 when he interned with the company while he was a computer science graduate student at the University of California, San Diego.

This research, like other projects Venkat leads, is funded by the National Science Foundation and Defense Advanced Research Projects Agency.

Venkat is also one of the university researchers who co-authored a paper with collaborators Mohammadkazem Taram and Tullsen from UC San Diego that introduce a more targeted microcode-based defense against Spectre. Context-sensitive fencing, as it is called, allows the processor to patch running code with speculation fences on the fly.

Introducing one of just a handful more targeted microcode-based defenses developed to stop Spectre in its tracks, "Context-Sensitive Fencing: Securing Speculative Execution via Microcode Customization" was published at the ACM International Conference on Architectural Support for Programming Languages and Operating Systems in April 2019. The paper was also selected as a top pick among all computer architecture, computer security, and VLSI design conference papers published in the six-year period between 2014 and 2019.

The new Spectre variants Venkat's team discovered even break the context-sensitive fencing mechanism outlined in Venkat's award-winning paper. But in this type of research, breaking your own defense is just

another big win. Each security improvement allows researchers to dig even deeper into the hardware and uncover more flaws, which is exactly what Venkat's research group did.