Crypto News

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

November 1, 2020

Contents

October 2020

30 Oct 2020

1 World's record entanglement storage

https://www.swissquantumhub.com/worlds-record-entanglement-storage/

Researchers from Sorbonne University in Paris have achieved a highly efficient transfer of quantum entanglement into and out of two quantum memory devices. This achievement brings a key ingredient for the scalability of a future quantum internet.

The team at Kastler Brossel Laboratory (Sorbonne Université, CNRS, ENS-Université PSL, Collège de France) demonstrated the storage and retrieval of entangled light beams into two quantum memory devices, with an overall efficiency as high as 85%. This value constitutes more than a three-fold increase relative to prior works in the field.

The experiment involved a very elongated ensemble of laser-cooled cesium atoms and was based on the protocol called electromagnetically induced transparency. A control laser beam makes the medium transparent and slows down the impinging signal light carrying the information. When the signal is contained within the ensemble and the control beam is turned off, the information is converted into a collective excitation of the atoms, which is stored until the control beams is turned on again. The team first generated two light beams that are entangled and then mapped them into two memories following this protocol. By using specific atomic transitions and reaching a very large absorption in each memory, the researchers were able to write and read out the entanglement with unprecedented efficiency, while preserving a very low noise contamination.

2 Quantum-computing pioneer warns of complacency over Internet security

by Davide Castelvecchi

https://www.nature.com/articles/d41586-020-03068-9

When physicists first thought up quantum computers in the 1980s, they sounded like a nice theoretical idea, but one probably destined to remain on paper. Then in 1995, 25 years ago this month, applied mathematician Peter Shor published a paper[1] that changed that perception.

Shor's paper showed how quantum computers could overcome a crucial problem. The machines would process information as qubits – quantum versions of ordinary bits that can simultaneously be '0' and '1'. But quantum states are notoriously vulnerable to noise, leading to loss of information. His error-correction technique – which detects errors caused by noise – showed how to make quantum information more robust.

Shor, who is now at the Massachusetts Institute of Technology in Cambridge and is also a published poet, had shocked the physics and computer-science worlds the previous year, when he found[2] the first potentially useful – but ominous – way to use a hypothetical quantum computer. He'd written an algorithm that would allow a quantum computer to factor integer numbers into prime factors at lightning speed. Most

[1] Shor, P. W. Phys. Rev. A 52, R2493(R) (1995).

[2] Shor, P. W. Proc. 35th Annual Symp. Found. Comp. Sci. 124–134 (1994).

Internet traffic today is secured by encryption techniques based on large prime numbers. Cracking those codes is hard because classical computers are slow at factoring large products.

Quantum computers are now a reality, although they are still too rudimentary to factor numbers of more than two digits. But it is only a matter of time until quantum computers threaten Internet encryption.

Nature caught up with Shor to ask him about the impact of his work – and where Internet security is heading.

Before your factoring algorithm, were quantum computers mostly a theoretical curiosity?

My paper certainly gave people an idea that these machines could do something useful. Computer scientist Daniel Simon, in a precursor of my result, solved a problem that he came up with that shows that quantum computers are exponentially faster [than ordinary computers]. But even after Simon's algorithm, it wasn't clear that they could do something useful.

What was the reaction to your announcement of the factoring algorithm?

At first, I had only an intermediate result. I gave a talk about it at Bell Labs [in New Providence, New Jersey, where I was working at the time] on a Tuesday in April 1994. The news spread amazingly fast, and that weekend, computer scientist Umesh Vazirani called me. He said, "I hear you can factor on a quantum computer, tell me how it works." At that point, I had not actually solved the factoring problem. I don't know if you know the children's game 'telephone', but somehow in five days, my result had turned into factoring as people were telling each other about it. And in those five days, I had solved factoring as well, so I could tell Umesh how to do it.

All sorts of people were asking me for my paper before I had even finished writing it, so I had to send them an incomplete draft.

But many experts still thought that quantum computers would lose information before you can actually finish your computation?

One of the objections was that in quantum mechanics, if you measure a system, you inevitably disturb it. I showed how to measure the error without measuring the computation – and then you can correct the error and not destroy the computation.

After my 1995 paper on error correction, some of the sceptics were convinced that maybe quantum computing might be doable.

Error correction relies on 'physical' and 'logical' qubits. What is the difference?

When you write down an algorithm for a quantum computer, you assume that the qubits are noiseless; these noiseless qubits that are described by the algorithm are the logical qubits. We actually don't have noiseless qubits in our quantum computers, and in fact, if we try to run our algorithm without any kind of noise reduction, an error will almost inevitably occur.

A physical qubit is one of the noisy qubits in our quantum computer. To run our algorithm without making any errors, we need to use the physical qubits to encode logical qubits, using a quantum error-correcting code. The best way we know how to do this has a fairly large overhead, requiring many physical qubits for each logical qubit.

It is quite complicated to work out how many more qubits are needed for the technique. If you want to build a quantum computer using surface code – the best candidate right now – for every logical qubit, you need about 100 physical qubits, maybe more.

In 2019, Google showed that its 54-qubit quantum computer could solve a problem that would take impossibly long on a classical computer – the first demonstration of a 'quantum advantage'. What was your reaction?

It's definitely a milestone. It shows that quantum computers can do things better than classical computers – at least, for a very contrived problem. Certainly some publicity was involved on Google's part. But also they have a very impressive quantum computer. It still needs to be a lot better before it can do anything interesting. There's also the startup IonQ. It looks like they can build a quantum computer that in some sense is better than Google's or IBM's.

When quantum computers can factor large prime numbers, that will enable them to break 'RSA' – the ubiquitous Internet encryption system.

Yes, but the first people who break RSA either are going to be NSA or some other big organization. At first, these computers will be slow. If you have a computer that can only break, say, one RSA key per hour, anything that's not a high priority or a national-security risk is not going to be broken. The NSA has much more important things to use their quantum computer on than reading your e-mail – they'll be reading the Chinese ambassador's e-mail.

Are there cryptography systems that can replace RSA and that will be secure even in the age of quantum computers – the 'post-quantum encryption'?

I think we have post-quantum cryptosystems that you could replace RSA with. RSA is not the big problem right now. The big problem is that there are other ways to break Internet security, such as badly programmed software, viruses, sending information to some not entirely honest player. I think the only obstruction to replacing RSA with a secure post-quantum cryptosystem will be will-power and programming time. I think it's something we know how to do; it's just not clear that we'll do it in time.

Is there a risk we'll be caught unprepared?

Yes. There was an enormous amount of effort put into fixing the Year 2000 bug. You'll need an enormous amount of effort to switch to post-quantum. If we wait around too long, it will be too late.

29 Oct 2020

3 How China hopes to win the quantum technology race

by Stephen Chen

https://www.scmp.com/news/china/science/article/3107640/how-china-hopes-win-quantum-technology-race

China's national quantum programme has been shrouded in secrecy until recently, when it was defined as part of the national strategy.

Britain, the European Union and the United States have all published plans in recent years to take a lead role in the global race on quantum science and technology.

China started work on a massive quantum research facility in Hefei in Anhui province three years ago, which has been designated as the headquarters of its national programme.

State media has reported the investment in the programme will reach 100 billion yuan (US$14.8 billion) by 2022, but no further information was disclosed to the public.

But earlier this month President Xi Jinping met some of the country's top quantum physicists and told them that the programme was part of the national strategy as the world underwent "the biggest change in a century".

He said quantum research would be "an advance-handed piece on the board" – a reference to the ancient Chinese game Go, in which a piece placed on a seemingly irrelevant area at the beginning of the game can help score victory at the end.

Quantum technology is one of the most complicated areas of physics exploring the behaviour of subatomic particles and has the potential to overturn the fundamental laws established by Newton and Einstein.

It relies on discoveries like the knowledge that two particles that are entangled will remain connected no matter how far apart they are, with changes in one affecting the behaviour of others.

In an article published in Science and Technology Daily soon after Xi's speech, Pan Janwei, the father of China's quantum satellite programme, said the county was trying to develop three disruptive technologies.

Quantum sensor

The first is a technology that will detect or measure physical disturbances with unprecedented sensitivity and precision.

Applications include airborne sensors that can reveal a submarine hiding hundreds of metres under the ocean, or guiding devices that can operate independently for months without a GPS signal.

Pan believes that China is currently lagging behind the US in this field.

Quantum computer

However, the two countries are running neck-and-neck in the race to develop superfast calculation machines.

A calculation that may take a present-day high-performance computer thousands of years to solve – for example guessing a password – may take only a few seconds on a quantum computer.

Quantum internet

The third technology is one that will lead to ultra-secure communication that uses entangled particles to transmit messages.

In theory it should prevent eavesdropping because attempts to hack messages will cause changes in the particles that will alert the users.

China has already built the world's first quantum satellite and longest quantum communication networks, putting it ahead of the United States, according to Pan.

4 Honeywell Releases Next Generation of Quantum Computer, Offers Glimpse Into Corporate Customers

by Matt Swayne

https://thequantumdaily.com/2020/10/29/honeywell-releases-next-generation-of-quantum-computer-offers-glimpse-into-corporate-customers/

Honeywell today announced its next-generation quantum computer, **the System Model H1**, today, according to a news release. The H1 generation of computer features Honeywell's differentiated quantum charge-coupled device (QCCD) trapped-ion technology and is strategically designed to be rapidly upgraded throughout its lifetime.

It's a 10-qubit computer that has registered a proven quantum volume of 128, according to the release. The machine continues to place Honeywell among the leaders in producing a commercial quantum computer, the president of the company's quantum solutions division said.

"Honeywell's aggressive quantum computing roadmap reflects our commitment to achieving commercial scale for our quantum business. Our subscription-based model provides enterprise customers with access to Honeywell's most advanced system available," said Tony Uttley, President of Honeywell Quantum Solutions. "Honeywell's unique methodology enables us to systematically and continuously 'upgrade' the H1 generation of systems through increased qubit count, even higher fidelities and unique feature modifications."

Uttley offered an analogy: "Imagine if the streaming service to which you subscribed became twice as good in a few weeks, 10 times as good in a few months and thousands of times better in a few quarters," he said.

The company offered a list of the latest enterprise companies with access to its quantum computer. That list includes DHL and Merck as well as a collaboration with Accenture. These companies demonstrate the wide range of quantum computing use cases, which include pharmaceuticals and logistics as well as Honeywell's own internal applications in its Aerospace and Performance Materials and Technologies businesses. Honeywell's differentiated technology, exemplified by the high-fidelity quantum operations and fully connected qubits with mid-circuit measurement and qubit reuse, enables customers to push the frontier of quantum computing applications.

"We believe that addressing tomorrow's global logistics challenges requires an unwavering commitment to advancing some of today's most promising technologies, and that includes Quantum Computing. By attempting to solve computationally complex problems with Honeywell, we have taken another step towards exploring improving operational efficiencies and leveraging quantum computing's potential to innovate within the logistics industry," said Justin Baird, head of innovation, Asia Pacific, for DHL Customer Solutions & Innovation.

Kam Chana, director, computational platforms at Merck said, "It was illuminating to experience the properties of real quantum hardware first-hand through Zapata's Orquestra platform. Seeing one of

Orquestra's native QML algorithms run on Honeywell's H1 system was an exciting moment for Merck in our journey to quantum readiness. The combination of Orquestra's programming environment with quantum hardware opens up quantum computing widely to our data scientists and brings new approaches for development of AI/ML based models."

Honeywell is also collaborating with Accenture on new use cases for Honeywell's quantum technology.

"At Accenture, we're excited to be working with quantum industry leaders as well as our clients to unlock new value through quantum computing," said Marc Carrel-Billiard, senior managing director and Technology Innovation lead at Accenture. "Working with Honeywell in this rapidly-developing space has already yielded new insights, and we look forward to exploring ways that the System Model H1 can be applied to business challenges across industries."

In addition, JPMorgan Chase has continued its collaboration with the Honeywell team. "JPMorgan Chase is pleased to continue innovating alongside Honeywell and its new System Model H1 quantum computer," says Dr. Marco Pistoia, head of research and engineering, JPMorgan Chase.

Quantum Volume of 128

The newest generation quantum computer from Honeywell initially offers 10 fully connected qubits, a proven quantum volume of 128 (the highest measured in the industry) and unique features such as mid-circuit measurement and qubit reuse, which were made possible through Honeywell's heritage of precision controls expertise. This announcement further affirms the company's commitment to rapidly increase quantum volume by at least an order of magnitude annually for the next five years.

System Model H1 is directly accessible to enterprises via a cloud application programming interface (API), as well as through Microsoft Azure Quantum, and alongside channel partners including Zapata Computing and Cambridge Quantum Computing. Access to System Model H1 is through a subscription that provides customers access to Honeywell's most technologically advanced quantum computer on the market.

In addition to the announced H1 computer, Honeywell confirmed it has already begun integration activities for its future System Model H2 generation, as well as development activities in support of its H3 generation and beyond.

Honeywell's novel trapped-ion qubits can be uniformly generated with errors better understood compared with alternative qubit technologies that do not use individual atoms. These high-performance operations require deep experience across multiple disciplines, including atomic physics, optics, cryogenics, lasers, magnetics, ultra-high vacuum, and precision control systems – areas where Honeywell has a long heritage of experience and expertise.

"The introduction of the System Model H1 is a significant milestone in shaping and accelerating the development of quantum computing and bringing its power to enterprises," added Uttley. "We've seen demand skyrocket in 2020 and are thrilled to partner with customers seeking to solve real business problems via quantum computing."

Honeywell currently has a cross-disciplinary team of more than 150 scientists, engineers, software developers and functional professionals dedicated to advancing quantum computing and addressing real enterprise problems across industries.

28 Oct 2020

5 NSA: We've learned our lesson after foreign spies used one of our crypto backdoors – but we can't say how exactly

by Thomas Claburn

https://www.theregister.com/2020/10/28/nsa_backdoor_wyden/

It's said the NSA drew up a report on what it learned after a foreign government exploited a weak encryption scheme, championed by the US spying agency, in Juniper firewall software.

However, curiously enough, the NSA has been unable to find a copy of that report.

On Wednesday, Reuters reporter Joseph Menn published an account of US Senator Ron Wyden's efforts to determine whether the NSA is still in the business of placing backdoors in US technology products.

Wyden (D-OR) opposes such efforts because, as the Juniper incident demonstrates, they can backfire, thereby harming national security, and because they diminish the appeal of American-made tech products.

But Wyden's inquiries, as a member of the Senate Intelligence Committee, have been stymied by lack of cooperation from the spy agency and the private sector. In June, Wyden and various colleagues sent a letter to Juniper CEO Rami Rahim asking about "several likely backdoors in its NetScreen line of firewalls."

Juniper acknowledged in 2015 that "unauthorized code" had been found in ScreenOS, which powers its NetScreen firewalls. It's been suggested that the code was in place since around 2008.

The Reuters report, citing a previously undisclosed statement to Congress from Juniper, claims that the networking biz acknowledged that "an unnamed national government had converted the mechanism first created by the NSA."

Wyden staffers in 2018 were told by the NSA that a "lessons learned" report about the incident had been written. But Wyden spokesperson Keith Chu told Reuters that the NSA now claims it can't find the file. Wyden's office did not immediately respond to a request for comment.

The reason this malicious code was able to decrypt ScreenOS VPN connections has been attributed to Juniper's "decision to use the NSA-designed Dual EC Pseudorandom Number Generator."

The company has yet to clarify exactly why it made that decision. Juniper did not respond to a request for comment.

When former NSA contractor Edward Snowden leaked agency secrets in 2013, Reuters reported that years earlier security firm RSA, now part of storage biz EMC, had accepted a $10m contract with the NSA to use Dual Elliptic Curve, or Dual EC, encryption. RSA at the time denied some of the claims without disputing the existence of the contract.

The NSA had been keen to see Dual EC adopted and worked with the US Commerce Department to promote it. But in 2007, two Microsoft researchers reported there were serious flaws with the Dual Elliptic Curve Deterministic Random Bit Generator that led it to produce weak cryptography. By 2014, US standards agency NIST withdrew support for Dual EC.

Juniper at some point between 2008 and 2009 appears to have added Dual EC support to its products at the request of "a single customer," widely believed to be the NSA.

After Snowden's disclosures about the extent of US surveillance operations in 2013, the NSA is said to have revised its policies for compromising commercial products. Wyden and other lawmakers have tried to learn more about these policies but they've been stonewalled, according to Reuters.

The NSA also declined to provide backdoor policy details to Reuters, stating that it doesn't share "specific processes and procedures." The news agency says three former senior intelligence officials have confirmed that NSA policy now requires a fallout plan with some form of warning in the event an implanted back door gets discovered and exploited.

6 First Trapped-Ion Quantum chip with integrated photonics

https://www.swissquantumhub.com/first-trapped-ion-quantum-chip-with-integrated-photonics/

Honeywell and IonQ both create trapped-ion qubits using an isotope of rare-earth metal called ytterbium. In its chip using integrated photonics, MIT used an alkaline metal called strontium. Strontium ions were used instead of ytterbium because strontium ions do not need UV light for optical control. A trapped-ion strontium quantum computer needs lasers of six different frequencies. Each frequency corresponds to a different color that ranges from near-ultraviolet to near-infrared. Each color performs a different operation on an ion qubit.

The process to create ions is essentially the same. Precision lasers remove an outer electron from an atom to form a positively charged ion. Then, lasers are used like tweezers to move ions into position. Once in position, oscillating voltage fields hold the ions in place. One main advantage of ions lies in the fact that it is natural instead of fabricated. All trapped-ion qubits are identical.

The current method of controlling lasers makes it challenging to build trapped-ion quantum computers beyond a few hundred qubits.

MIT researchers have figured out how to use optical fibers and photonics to carry laser pulses directly into the vacuum chamber and focus them on individual ions on the chip.

7 Zero Trust Cybersecurity: 'Never Trust, Always Verify'

by Alper Kerman

https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

Huh? What? At least that was my response the first time I heard the words "zero trust" when I started working at the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) in the fall of 2018. Mind you, I was also making a fresh start with an enormous jump to cybersecurity from a career track that had generally been in software engineering. Sure, I did design and develop secure software solutions and even put together secure systems and platforms at times throughout my career, but zero trust seemed like a different ballgame to me. For one thing, it didn't have a fence.

What do I mean by that? Well, the traditional approach to cybersecurity relies upon barriers – firewalls – that control traffic coming in and out of a network. Zero trust, on the other hand, is about assuming no barriers. It is usually mentioned in the same breath as "removing perimeters," "shrinking perimeters," "reducing perimeters" or "going perimeter-less." These are common references to the idea of "de-perimeterization," which was originally introduced by a group called the Jericho Forum back in 2005. Then in 2010, cybersecurity expert John Kindervag coined the phrase "zero trust" while he was with Forrester Research. In a nutshell, zero trust assumes that the system will be breached and designs security as if there is no perimeter. Hence, don't trust anything by default, starting with the network.

We'll get into what zero trust means for cybersecurity in a minute. But first, how did NCCoE – and I – get wrapped up in zero trust? Well, it's kind of a long story.

A Big Breach Starts the Ball Rolling

I will dare to argue that the coup de grâce was the Office of Personnel Management (OPM) data breach of 2015. An estimated 22.1 million records were exposed! And if you aren't shaking your head right about now, you should be, as it has been described as one of the largest breaches of U.S. government data in history. It exposed records of people who had undergone background checks, as well as information about their family, friends and acquaintances, many of whom weren't even government employees. Social Security numbers, names, dates and places of birth, and addresses were among the types of personally identifiable information that were revealed.

The OPM data breach was a big wake-up call for the U.S. government to secure its information systems and infrastructures. In its aftermath, several initiatives were launched to improve and modernize the U.S. government's security posture. The American Technology Council, formed in May 2017 under the direction of the president, promptly coordinated and produced a report for federal IT modernization later that year.

Then, a year later in February 2018, the CIO Council Services, Strategy, and Infrastructure Committee, made up of federal IT officers, chartered the Zero Trust and Software-Defined Networking Steering Group. That group's job was to support the adoption of more effective methods and technologies for verifying, securing, enforcing and continuously monitoring access to the federal government's assets and data by applying zero trust principles. The group convened a workshop on October 25, 2018, at the NCCoE. The workshop included 21 representatives and subject matter experts from federal civilian and defense agencies alike to discuss and come to consensus on definitions of zero trust networking and software-defined networking, including components, functional capabilities and security characteristics of each model. Shortly after the workshop, I came to work at NIST/NCCoE and was asked to participate in the steering group meetings as the new technical lead. This interaction finally led to the February 2019 launching of a NIST NCCoE project in partnership with the CIO Council to research zero trust and zero trust architectures (ZTA) with the goal to produce a general guidance document for adoption of ZTAs for securing U.S. government information systems and infrastructures.

In August 2020, NIST NCCoE released the general guidance document NIST SP 800-207, Zero Trust Architecture, for adoption of ZTAs in the federal government. This is a document that provides conceptual-level insight for zero trust and zero trust architectures, including deployment models, use case scenarios and discovered gaps in technologies.

Now, with the historical backdrop out of the way, let's refocus our attention on our main topic: zero trust and what it means for cybersecurity.

Keeping Networks Safe, Then and Now

The best way to quickly get your mind wrapped around zero trust is to consider traditional and present network environments. People who have been in the IT field since the earliest days will surely remember the more innocent times in which we put together network environments. They were immensely different to say the least, as we didn't have remotely accessible resources or applications and services in the cloud like we do today. Sure, we used digital resources and applications to do our work; however, they were exclusive to internal networks and accessible to staff who were on PCs and laptops within those network environments. How did we protect them from internet threats? We threw a digital fence – a perimeter – around them, which funneled external accesses through a single point of entry in a verified and authorized manner. This would allow the internal users access to the pool of resources and applications protected inside the perimeter. And this was a sound strategy for a long time.

Today, with the explosion of cloud computing, we are more globally connected than ever before. Most of us conduct business remotely using mobile devices. We consume, exchange and store digital information in private clouds, public clouds, hybrid clouds and many other variations in between. Needless to say, the conventional boundaries have expanded and become more obscured to allow for a much larger footprint of applications and services to be located and accessed from anywhere. Of course, with that expansion, the cybersecurity vulnerabilities have also grown. We now have more areas and points of attack. And we are especially vulnerable to the types of cybersecurity breaches that originate from inside the networks – inside the perimeter.

In fact, in the case of infamous OPM data breach I mentioned above, hackers first gained access to OPM's internal network using stolen credentials and then planted a malware package that installed itself within OPM's network as a back door for data exfiltration. From there, attackers escalated their privileges to gain access to various OPM information systems, a typical escalation scenario that is often referred to as the "lateral movement" or "East-West traffic" of a security breach inside the perimeter. The shortcoming with the conventional perimeter defense is that it provides no security control mechanism to prevent lateral movements once the security threat is inside the perimeter, as inside is always considered to be the safe or trusted zone in this strategy.

This is where zero trust comes in to save the day. You could be working from an enterprise-owned network, a coffee shop, home or anywhere in the world, accessing resources spread across many boundaries, from on-premises to multiple cloud environments. Regardless of your network location, a zero trust approach to cybersecurity will always respond with, "I have zero trust in you! I need to verify you first before I can trust you and grant access to the resource you want." Hence, "never trust, always verify" – for every access request!

And to stress the point further, the verification process is one of the key aspects of zero trust approach. Every access request to a resource must be thoroughly evaluated dynamically and in real time based on access policies in place and current state of credentials, device, application and service, as well as other observable behavior and environmental attributes, before access may be granted. For example, a member of staff or a contractor, or even a guest user, may be verified and granted access to a specific resource, but they will still need to be reverified to access another resource within a zero-trust-enforced environment. This continuous scrutiny is the security control mechanism that prevents lateral movement of bad actors spreading from compromised systems within network environments, which is basically the essence of any zero trust solution.

I've had many amazing working experiences throughout my career, but I have to admit, this experience with our zero trust efforts at NIST/NCCoE definitely tops the chart by far. And whats really even more gratifying is that our zero trust efforts are being closely followed and highly regarded by other government agencies and many in the industry. And for that, all the kudos go to every member of my team for their awesome support in our zero trust efforts and activities.

27 Oct 2020

8 How Can AI And Quantum Computers Work Together?

by Gary Fowler

https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/10/27/how-can-ai-and-quantum-computers-work-together/#4b65154c6ad1

Traditional computers operate based on data that is encoded in a binary system. Essentially, each bit of data is represented in zeroes and ones only – no more, no less than the two forms. Hence, the binary computing system. However, there is a new generation of computers emerging on the horizon called quantum computing and it's taking computing systems beyond the normal binary.

Instead of just the zeroes and the ones, quantum computing depends on quantum bits or qubits. Quantum computing breaks the boundaries of traditional computing by allowing the information – coded in qubits – to have multiple states at once. This phenomenon, known as superposition, unlocks more computing power than previously imagined. With such a complicated background story, where does the use of quantum computing make the most sense in the current context and what benefits does it offer practically?

No doubt, the technology is still in the early stages of development, but despite the novelty of the innovation, there is a shortlist of tech mammoths in line to invest in it. Companies like IBM, Google and Microsoft have taken initial steps to invest in and adopt quantum computing.

One of the areas where quantum computing is more lucrative and promising is artificial intelligence. As AI operates on the analysis of large datasets, the margin of error and inaccuracy in the process of learning has significant room for improvement – and quantum computing may well allow us to improve the algorithm's ability to learn and interpret.

How does quantum computing exactly help in artificial intelligence and more specifically, in machine learning? The truth is modern-day machine learning's extent of efficiency and success largely depends on the dataset it's given. The size of the dataset determines the quality of the results, so if the information isn't ample, the output won't be promising either. However, thanks to quantum computing's ability to go beyond the traditional binary coding system, it makes it possible to enlarge and enrich the data set, both in terms of volume and diversity. With better and more in-depth datasets, it becomes possible to better train machine learning models, which can then contribute to real-life problem-solving.

Another enhancement that quantum computing introduces to AI is the improvement of "natural language processing" capabilities that allow for a more in-depth understanding and analysis of textual data. With quantum computing, the algorithms can become more aware of the content of the textual data. In other words, the machine will be able to truly understand the meaning behind the data, being able to analyze whole sentences and phrases instead of just words.

When it comes to the industry-specific impact that quantum computing can render, the list of advantages it introduces is also long and very well possible in the near future. Some of the most promising breakthroughs quantum computing offers is in health care. Since traditional computers are limited in the amount of data they can hold and analyze, quantum computing steps in to expand the sheer size and variety of various molecules available for research and comparison. As the process of molecule simulation and comparison is the backbone of any drug development initiative, quantum computing will push the boundaries of medical research by allowing for more informed and diverse simulations designed to test the interactions between drugs and human body molecules. In addition to research, quantum computing can improve capacities for pattern recognition, create enlarged data sets and improve MRI image accuracy thereby allowing medical professionals to diagnose and treat conditions sooner.

Similar to diagnostics in health care, quantum computing will unlock new capabilities in the finance industry. Specifically, with fraud detection, which relies largely on pattern recognition. Quantum computers can help detect fraud early on and significantly increase the speed of analysis thanks to its improved power and capacity.

Beyond health care and finance, quantum computing will also completely redefine marketing practices in place today. With enlarged consumer data sets and analysis capabilities, brands and companies will be able to introduce a completely new level of customization to meet the needs of individual customers and users. Quantum computing will make it possible to target customers on a much more granular level, developing communication campaigns that accurately meet – and anticipate – customer needs and preferences.

By enhancing AI's ability to analyze and learn based on data sets, quantum computing will eliminate the main concerns about data quality and analysis accuracy that still serve as obstacles in the application process of machine learning algorithms in various scenarios. Even though quantum computing needs more time to find full integration and adoption across industries today, the possibilities it may introduce are, by all means, revolutionary and promising.

26 Oct 2020

9 Surprising communication between atoms could improve quantum computing

by Sarah Perdue

https://phys.org/news/2020-10-atoms-quantum.html

A group of University of Wisconsin-Madison physicists has identified conditions under which relatively distant atoms communicate with each other in ways that had previously only been seen in atoms closer together – a development that could have applications to quantum computing.

The physicists' findings, published Oct. 14 in the journal Physical Review A, open up new prospects for generating entangled atoms, the term given to atoms that share information at large distances, which are important for quantum communications and the development of quantum computers.

"Building a quantum computer is very tough, so one approach is that you build smaller modules that can talk to each other," says Deniz Yavuz, a UW-Madison physics professor and senior author of the study. "This effect we're seeing could be used to increase the communication between these modules."

The scenario at hand depends on the interplay between light and the electrons that orbit atoms. An electron that has been hit with a photon of light can be excited to a higher energy state. But electrons loathe excess energy, so they quickly shed it by emitting a photon in a process known as decay. The photons atoms release have less energy than the ones that boosted the electron up – the same phenomenon that causes some chemicals to fluoresce, or some jellyfish to have a green-glowing ring.

"Now, the problem gets very interesting if you have more than one atom," says Yavuz. "The presence of other atoms modifies the decay of each atom; they talk to each other."

If a single atom decays in one second, for example, then a group of the same type of atom may decay in less – or more – than one second. The timing depends on the conditions, but all the atoms decay at the same rate, either more quickly or more slowly. So far, this type of correlation has only been observed if the atoms are within about one wavelength of the emitted light from each other. For rubidium atoms, used by Yavuz and his colleagues, it means within 780 nanometers – right at the edge between the wavelength of red and infrared light.

The scientists wanted to see how greater distances between the atoms would affect the decay of rubidium atoms. If the prevailing idea were correct, then two rubidium atoms further apart than 780 nanometers would act like individual atoms, each giving the characteristic single-atom decay profile.

In their experiments, they first immobilized a group of rubidium atoms by laser-cooling them to just slightly above absolute zero, the temperature at which atomic motion ceases. Then, they shined a laser at rubidium's excitation wavelength to energize electrons, which decay while emitting a photon at the characteristic 780 nm. They could then measure the intensity of that emitted photon over time and compare it to the decay profile of a single rubidium atom.

"In our case, we showed that the atoms can be as far away as five times the wavelength, and still these group effects are pronounced – the decay can be faster than if the atom were there by itself, or slower," Yavuz says. "The second thing we showed is, if you look at the time dynamics of the decay, it can start fast and then get slower. It switches, and that switch had never been seen before."

With these new insights into building correlations between atoms, Yavuz and his research group are looking into the quantum computing applications of their findings. They are investigating which experimental conditions lead to different types of correlated states, which can lead to entanglement and efficient transmission of quantum information.

22 Oct 2020

10 Intel Creating Cryptographic Codes That Quantum Computers Can't Crack

by Jeremy Hsu

https://spectrum.ieee.org/tech-talk/computing/hardware/how-to-protect-the-internet-of-things-in-the-quantum-computing-era

The world will need a new generation of cryptographic algorithms once quantum computing becomes powerful enough to crack the codes that protect everyone's digital privacy. An Intel team has created an improved version of such a quantum-resistant cryptographic algorithm that could work more efficiently on the smart home and industrial devices making up the Internet of Things.

The **Bit-flipping Key Encapsulation (BIKE)** provides a way to create a shared secret that encrypts sensitive information exchanged between two devices. The encryption process requires computationally complex operations involving mathematical problems that could strain the hardware of many Internet of Things (IoT) devices. But Intel researchers figured out how to create a hardware accelerator that enables the BIKE software to run efficiently on less powerful hardware.

"Software execution of BIKE, especially on lightweight IoT devices, is latency and power intensive," says Manoj Sastry, principal engineer at Intel. "The BIKE hardware accelerator proposed in this paper shows feasibility for IoT-class devices."

Intel has been working in cooperation with several other companies to develop BIKE as one possible quantum-resistant algorithm among the many being currently evaluated by the U.S. National Institute of Standards and Technology. This latest version of BIKE developed primarily by the Intel team was presented in a paper during the IEEE International Conference on Quantum Computing and Engineering on 13 October 2020.

BIKE securely establishes a shared secret between two devices through a three-step process, says Santosh Ghosh, a research scientist at Intel and coauthor on the paper. First, the host device creates a public-private key pair and sends the public key to the client. Second, the client sends an encrypted message using the public key to the host. And third, the host decodes the encrypted message through a BIKE decode procedure using the private key. "Of these three steps, BIKE decode is the most compute intensive operation," Ghosh explains.

The improved version of BIKE takes advantage of a new decoder that requires less computing power. Testing showed that this enabled the computation of a single BIKE decode operation in 1.3 million cycles at 110 MHz on an Intel Arria 10 FPGA in 12 milliseconds, which is fairly competitive compared to other options.

"BIKE is well suited for applications where IoT devices are used for encapsulation and a more capable device takes the role of host to generate the keys and perform the decapsulation procedure," Ghosh says.

This also represents the first hardware implementation of BIKE suitable for Level 5 keys and ciphertexts, with level 5 representing the highest level of security as defined by the U.S. National Institute of Standards and Technology. Each higher level of security requires bigger keys and ciphertexts – the encrypted forms of data that would look unintelligible to prying eyes – which in turn require more compute-intensive operations.

The team was previously focused on BIKE implementations suitable for the lower security levels of 1 and 3, which meant the public hardware implementation submitted to NIST as reference did not support level 5, says Rafael Misoczki, coauthor on the paper who was formerly at Intel and is now a cryptography engineer at Google.

The latest hardware implementation for BIKE takes the security up a couple of notches.

"Our BIKE decoder supports keys and ciphertexts for Level 5 which provides security equivalent to AES-256," says Andrew Reinders, security researcher at Intel and coauthor on the paper. "This means a quantum computer needs 2^{128} operations to break it."

The latest version of the BIKE hardware accelerator has a design that offers additional security against side-channel attacks in which attackers attempt to exploit information about the power consumption or even timing of software processes. For example, differential power analysis attacks can track the power consumption patterns associated with running certain computational tasks to reveal some of the underlying computations.

In theory, such attacks against BIKE might attempt to target a small block of the secret being shared between two devices. That block size depends upon how many secret bits work together in underlying sub-operations, Reinders says. Because a BIKE block size is 1-bit, a BIKE hardware design that processed a single secret bit at a time would be highly vulnerable to such a differential power analysis attack.

But the new BIKE hardware accelerator offers protection against such attacks because it performs all the computations for the 128-bits of secret in parallel, which makes it difficult to single out power consumption patterns associated with individual computations.

The BIKE hardware accelerator also has protection against timing attacks, because its decoder always runs for a fixed number of rounds that are each the same amount of time.

BIKE was previously chosen as one of eight alternates in the third round of NIST's Post-Quantum Cryptography Standardization Process that is currently narrowing down the best candidates to replace modern cryptography standards. Seven other algorithms were selected as finalists, making for a total of 15 algorithms remaining under consideration from a starting group of 69 submissions.

The researchers have submitted their revised version of BIKE for the third round of the NIST challenge and are currently awaiting comments. If all goes well, the federal agency plans to release the initial standard for quantum-resistant cryptography in 2022.

11 Optical wiring for large quantum computers

by Oliver Morsch

https://phys.org/news/2020-10-optical-wiring-large-quantum.html

Researchers at ETH have demonstrated a new technique for carrying out sensitive quantum operations on atoms. In this technique, the control laser light is delivered directly inside a chip. This should make it possible to build large-scale quantum computers based on trapped atoms.

Hitting a specific point on a screen with a laser pointer during a presentation isn't easy – even the tiniest nervous shaking of the hand becomes one big scrawl at a distance. Now imagine having to do that with several laser pointers at once. That is exactly the problem faced by physicists who try to build quantum computers using individual trapped atoms. They, too, need to aim laser beams – hundreds or even thousands of them in the same apparatus – precisely over several meters such as to hit regions only a few micrometers in size that contain the atoms. Any unwanted vibration will severely disturb the operation of the quantum computer.

At ETH in Zurich, Jonathan Home and his co-workers at the Institute for Quantum Electronics have now demonstrated a new method that allows them to deliver multiple laser beams precisely to the right locations from within a chip in such a stable manner that even the most delicate quantum operations on the atoms can be carried out.

Aiming for the quantum computer

To build quantum computers has been an ambitious goal of physicists for more than thirty years. Electrically charged atoms – ions – trapped in electric fields have turned out to be ideal candidates for the quantum bits or qubits, which quantum computers use for their calculations. So far, mini computers containing around a dozen qubits could be realized in this way. "However, if you want to build quantum computers with several thousand qubits, which will probably be necessary for practically relevant applications, current implementations present some major hurdles," says Karan Mehta, a postdoc in Home's laboratory and first author of the study recently published in the scientific journal Nature. Essentially, the problem is how to send laser beams over several meters from the laser into a vacuum apparatus and eventually hit the bull's eye inside a cryostat, in which the ion traps are cooled down to just a few degrees above absolute zero in order to minimize thermal disturbances.

Optical setup as an obstacle

“Already in current small-scale systems, conventional optics are a significant source of noise and errors – and that gets much harder to manage when trying to scale up”, Mehta explains. The more qubits one adds, the more complex the optics for the laser beams becomes which is needed for controlling the qubits. “This is where our approach comes in”, adds Chi Zhang, a Ph.D. student in Home’s group: “By integrating tiny waveguides into the chips that contain the electrodes for trapping the ions, we can send the light directly to those ions. In this way, vibrations of the cryostat or other parts of the apparatus produce far less disturbance.”

The researchers commissioned a commercial foundry to produce chips which contain both gold electrodes for the ion traps and, in a deeper layer, waveguides for laser light. At one end of the chips, optical fibers feed the light into the waveguides, which are only 100 nanometres thick, effectively forming optical wiring within the chips. Each of those waveguides leads to a specific point on the chip, where the light is eventually deflected towards the trapped ions on the surface.

Work from a few years ago (by some of the authors of the present study, together with researchers at MIT and MIT Lincoln Laboratory) had demonstrated that this approach works in principle. Now the ETH group has developed and refined the technique to the point where it is also possible to use it for implementing low-error quantum logic gates between different atoms, an important prerequisite for building quantum computers.

High-fidelity logic gates

In a conventional computer chip, logic gates are used to carry out logic operations such as AND or NOR. To build a quantum computer, one has make sure that it can to carry out such logic operations on the qubits. The problem with this is that logic gates acting on two or more qubits are particularly sensitive to disturbances. This is because they create fragile quantum mechanical states in which two ions are simultaneously in a superposition, also known as entangled states.

In such a superposition, a measurement of one ion influences the result of a measurement on the other ion, without the two being in direct contact. How well the production of those superposition states works, and thus how good the logic gates are, is expressed by the so-called fidelity. “With the new chip we were able to carry out two-qubit logic gates and use them to produce entangled states with a fidelity that up to now could only be achieved in the very best conventional experiments,” says Maciej Malinowski, who was also involved in the experiment as a Ph.D. student.

The researchers have thus shown that their approach is interesting for future ion trap quantum computers as it is not just extremely stable, but also scalable. They are currently working with different chips that are intended to control up to ten qubits at a time. Furthermore, they are pursuing new designs for fast and precise quantum operations that are made possible by the optical wiring.

20 Oct 2020

12 Beit Demonstrates Grover’s Search Algorithm on the Honeywell System Model H0

https://quantumcomputingreport.com/news/

Beit Inc. has released a paper showing they have implemented a range of unstructured search algorithms, scaling as well as coveted Grover's algorithm in lists of 16, 32 and 64 elements on a Honeywell's 6 qubit ion trap based quantum processor. This work follows a previous paper where they demonstrated a 16 element search on one of IBM's 5 qubit superconducting quantum processor. A measure that Beit uses is the probability of success as a function of the number of Oracle calls in the algorithm. By this measure, for the 16 and 32 element lists, Beit's quantum implementation beat out the probability of success a classical computer could achieve for the same number of oracle calls. And for the 16 element list, they achieved a higher probability of success with the ion trap machine (66%) than they previously achieved with the superconducting processor (24.5%). Although the number of elements in the lists are still small and the classical computer could quickly do much better with more oracle calls, this is an indication of future directions in their research.

13 Scientists Crack Quantum Physics Puzzle

by UNIVERSITY OF AUCKLAND

https://scitechdaily.com/scientists-crack-quantum-physics-puzzle/

Scientists have re-investigated a sixty-year-old idea by the American physicist P.W. Anderson and provided new insights into the quantum world.

Quantum physics explains how the world's building blocks such as atoms or electrons are put together. Everything we see around us is made up of atoms and electrons which are so small one billion atoms placed side by side could fit within a centimeter.

Because of the way atoms and electrons behave, scientists describe this behavior as waves. In the research, scientists looked at how waves can go through a landscape containing obstacles placed in random positions.

Anderson initially developed this idea to describe electrons in semiconductors. His insight greatly contributed to the development of computer chips and electronics.

"His work describes a common phenomenon that happens for all kinds of waves, be it light waves, ocean waves, sound waves or quantum-mechanical waves," says lead researcher Maarten Hoogerland from the University of Auckland.

Waves, unlike particles that travel in straight lines, can go around obstacles, but if there are enough random obstacles, the waves cannot get through because they interfere with each other and cancel themselves out.

In the Quantum Information Lab at the University, researchers took Anderson's work one step further and added an ultra-cold atom experiment to the mix. With the aid of high tech lasers, they manipulated these ultra-cold atoms until they were so cold, their wave behavior became visible to the eye.

"We are talking a billionth of a degree above absolute zero (-273.15 degrees C) so that is pretty chilly. We have created customized patterns of obstacles to stop the waves, and when we take a picture, we can find out where these atoms are," Dr Hoogerland says.

"This way, we can see what exactly is required to get our quantum-mechanical waves to reflect off obstacles, and why the waves do not get in."

Working together, through the Dodd-Walls Centre for Photonics and Quantum Technologies, with researchers at the University of Otago, the research team was able to match the results of the experiments with theoretical predictions, giving way to new insights which could be used to create and test “designer materials” with customized properties.

14 Quantum Monte Carlo Tree Search Framework for Quantum Circuit Transformation

https://www.swissquantumhub.com/quantum-monte-carlo-tree-search-framework-for-quantum-circuit-transformation/

In Noisy Intermediate-Scale Quantum (NISQ) era, quantum processing units (QPUs) suffer from, among others, highly limited connectivity between physical qubits.

To make a quantum circuit executable, a circuit transformation process is necessary to transform it into a functionally equivalent one so that the connectivity constraints imposed by the QPU are satisfied.

While several algorithms have been proposed for this goal, the overhead costs are often very high, which degenerates the fidelity of the obtained circuits sharply. One major reason for this lies in that, due to the high branching factor and vast search space, almost all these algorithms only search very shallowly and thus, very often, only (at most) locally optimal solutions can be reached.

Researchers at Southeast University, China and University of Technology Sydney propose a Monte Carlo Tree Search (MCTS) framework to tackle this problem, which enables the search process to go much deeper.

In particular, they have designed, by taking both short- and long-term rewards into consideration, a scoring mechanism. and propose to use a fast random strategy for simulation.

The thus designed search algorithm is polynomial in all relevant parameters and empirical results on extensive realistic circuits show that it can often reduce the size of output circuits by at least 30% when compared with the state-of-the-art algorithms on IBM Q20.

15 NSA publishes list of top vulnerabilities currently targeted by Chinese hackers

by Catalin Cimpanu

https://www.zdnet.com/article/nsa-publishes-list-of-top-25-vulnerabilities-currently-targeted-by-chinese-hackers/

The US National Security Agency has published today an in-depth report detailing the top 25 vulnerabilities that are currently being consistently scanned, targeted, and exploited by Chinese state-sponsored hacking groups.

All 25 security bugs (see the original article for details) are well known and have patches available from their vendors, ready to be installed.

Exploits for many vulnerabilities are also publicly available. Some have been exploited by more than just Chinese hackers, being also incorporated into the arsenal of ransomware gangs, low-level malware groups, and nation-state actors from other countries (i.e., Russia and Iran).

"Most of the vulnerabilities listed below can be exploited to gain initial access to victim networks using products that are directly accessible from the Internet and act as gateways to internal networks," the NSA said today.

The US cyber-security agency urges organizations in the US public and private sector to patch systems for the vulnerabilities.

16 Measuring Progress in the 'Noisy' Era of Quantum Computing

by Jeremy Hsu

https://spectrum.ieee.org/tech-talk/computing/hardware/measuring-progress-in-the-noisy-era-of-quantum-computing

Measuring the progress of quantum computers can prove tricky in the era of "noisy" quantum computing technology. One concept, known as "quantum volume," has become a favored measure among companies such as IBM and Honeywell. But not every company or researcher agrees on its usefulness as a yardstick in quantum computing.

In an ideal world, researchers could measure progress in quantum computing based on the number of quantum bits (qubits) in each system. But noise in the form of heat or electromagnetic sources constantly threatens to disrupt the computations among the fragile qubits, which makes it hard to reliably measure a quantum computer's capabilities based only upon the total number of qubits. That is why IBM researchers proposed the concept of quantum volume as a more reliable measure during this imperfect stage of quantum computing technology.

"Think of quantum volume as the average of worst-case circuits run on any quantum computer," says Jay Gambetta, a research fellow and vice president in quantum computing at IBM. "The result means that if this 'worst case' is possible, quantum volume is a measure of the circuits' quality; the higher the quality, the more complex circuits can be run on a quantum computer."

More specifically, IBM's team defines quantum volume as 2 to the power of the size of the largest circuit with equal width and depth that can pass a certain reliability test involving random two-qubit gates, says Daniel Lidar, director of the Center for Quantum Information Science and Technology at the University of Southern California in Los Angeles. The circuit's size is defined by either width based on the number of qubits or depth based on the number of gates, given that width and depth are equal in this case.

That means a 6-qubit quantum computing system would have a quantum volume of 2 to the power of 6, or 64 – but only if the qubits were relatively free of noise and the potential errors that can accompany such noise. (This is why the reliability test matters for the quantum volume definition.)

Lidar, who was not involved with coining the quantum volume concept, sees it as a useful measure for today's quantum computers that are described as Noisy Intermediate-Scale Quantum (NISQ) technology. "Such a metric is an excellent way to capture the performance of NISQ-era quantum computers, which define the era where noise still plays an important limiting factor in attaining high circuit depth with reliable performance," Lidar says.

Since IBM began publicizing the term more starting in late 2019, quantum volume has come up a number of times in the quantum computing papers and press releases of IBM and other companies such as Honeywell. But there is already at least one tech company CEO floating the idea that the end of quantum volume's usefulness might be in sight.

While discussing IonQ's latest quantum computing developments in an Ars Technica interview, CEO Peter Chapman talked about how improvements in the reduction of noise could effectively lead to a high-fidelity, 32-qubit system with a quantum volume of approximately 4 million. Within 18 months, he suggested, quantum volume numbers could grow so large that researchers might need to rethink the definition of quantum volume to retain its usefulness.

But Lidar disagrees that quantum volume is headed for relatively swift obsolescence. He points out that the quantum volume number would only grow so fast because of the "2 to the power" part of the definition. In fact, he adds, IBM did not even define quantum volume with the "2 to the power" part in its first paper on the subject back in 2017. "This is purely an artifact of this definition," Lidar says.

The simplest solution would be to define quantum volume in accordance with the largest number of qubits or gates, instead of using "2 to the power" of those numbers, Lidar says.

Not everyone sees quantum volume as a hugely important or necessary for benchmarking the progress of quantum computing. It's not clear if distilling quantum computing progress into a single measure is even necessary, says Scott Aaronson, a computer scientist and director of the Quantum Information Center at the University of Texas at Austin. He raised this and other questions in a blog post titled "Turn Down the Quantum Volume."

"It's basically just one possible 'gross consumer index of quantum computer awesomeness,' among countless alternatives that could be defined," Aaronson says.

For practical purposes, it's mostly big quantum computing industry players such as IBM that are currently concerned about quantum volume, says Javad Shabani, an assistant professor of physics and chair of the Shabani Lab at New York University. That's because he and other academic researchers generally don't have hardware access to such large quantum computing systems, even if more companies are offering cloud-based access to such systems for programming purposes.

Still, Shabani sees quantum volume as a useful concept that defines quantum computing progress in a more meaningful way than simply counting qubits. Like Lidar, he suggests that quantum volume will remain relevant as long as noise remains a limiting factor for quantum computers – whether that is the case for the next five years or the next decade or more.

"If you can make a logical qubit that basically has no noise, then slowly this quantum volume thing will go away naturally," Shabani says.

17 Scientists Say They Developed an Improved Fourier Transform for Quantum Computing

by Matt Swayne

https://thequantumdaily.com/2020/10/20/scientists-say-they-developed-an-improved-fourier-transform-for-quantum-computing/

Scientists say they have design a novel quantum circuit that calculates the fast Fourier transform, an indispensable tool in all fields of engineering, according to a news release.

The Fourier transform is a mathematical operation essential to virtually all fields of physics and engineering. Although an algorithm already exists that computes the Fourier transform in quantum computers, it is not versatile enough for many practical applications. In a recent study, scientists from Tokyo University of Science tackle this problem by designing a novel quantum circuit that calculates the

Fourier transform in a much quicker, versatile, and more efficient way.

The Fourier transform is an important mathematical tool that decomposes a function or dataset into its constituting frequencies, much like a musical chord can be decomposed into a combination of its notes. It is used across all fields of engineering in some form or another and, accordingly, algorithms to compute it efficiently have been developed-that is, at least for conventional computers. But what about quantum computers?

Though quantum computing remains an enormous technical and intellectual challenge, it has the potential to speed up many programs and algorithms immensely provided that appropriate quantum circuits are designed. In particular, the Fourier transform already has a quantum version called the quantum Fourier transform (QFT), but its applicability is quite limited because its results cannot be used in subsequent quantum arithmetic operations.

To address this issue, in a recent study published in Quantum Information Processing , scientists from Tokyo University of Science developed a new quantum circuit that executes the “quantum fast Fourier transform (QFFT)” and fully benefits from the peculiarities of the quantum world. The idea for the study came to Mr. Ryo Asaka, first-year Master’s student and one of the scientists on the study, when he first learned about the QFT and its limitations. He thought it would be useful to create a better alternative based on a variant of the standard Fourier transform called the “fast Fourier transform (FFT),” an indispensable algorithm in conventional computing that greatly speeds things up if the input data meets some basic conditions.

To design the quantum circuit for the QFFT, the scientists had to first devise quantum arithmetic circuits to perform the basic operations of the FFT, such as addition, subtraction, and digit shifting. A notable advantage of their algorithm is that no “garbage bits” are generated; the calculation process does not waste any qubits, the basic unit of quantum information. Considering that increasing the number of qubits of quantum computers has been an uphill battle over the last few years, the fact that this novel quantum circuit for the QFFT can use qubits efficiently is very promising.

Another merit of their quantum circuit over the traditional QFT is that their implementation exploits a unique property of the quantum world to greatly increase computational speed.

Associate Professor Kazumitsu Sakai, who led the study, explains: “In quantum computing, we can process a large amount of information at the same time by taking advantage of a phenomenon known as ‘superposition of states.’ This allows us to convert a lot of data, such as multiple images and sounds, into the frequency domain in one go.” Processing speed is regularly cited as the main advantage of quantum computing, and this novel QFFT circuit represents a step in the right direction.

The QFFT circuit is also much more versatile than the QFT.

“One of the main advantages of the QFFT is that it is applicable to any problem that can be solved by the conventional FFT, such as the filtering of digital images in the medical field or analyzing sounds for engineering applications,” said assistant professor Ryoko Yahagi, who also participated in the study.

19 Oct 2020

18 Toppan, NICT, QunaSys, and ISARA Launch Collaboration to Establish Quantum Secure Cloud Technology

by ISARA Corporation

https://www.toppan.com/en/news/2020/10/newsrelease201019e.html?utm_medium=email&_hsmi=98554624&_hsenc=p2ANqtz--AycvGA9hEctoFXgECy_N1L9e6U7V4gnbVfrTvSkTA-epW0gUAhZ01pPF9ZNZEAZL5tN9CFoslx0InheoZLhqj2B5LeQ&utm_content=98554624&utm_source=hs_email

Toppan Printing, the National Institute of Information and Communications Technology (NICT), QunaSys Corporation (QunaSys), and ISARA Corporation (ISARA) have announced the launch of a collaboration targeting the establishment of quantum secure cloud technology that will enable advanced information processing and secure communication, storage, and use of data.

Quantum secure cloud technology fuses quantum cryptography and secret sharing technologies to facilitate secure data communication, storage, and use. The establishment of the technology will not only ensure a high level of security that makes tampering and decryption impossible, but will also enable the collection, analysis, processing, and use of highly sensitive personal and corporate information accumulated in such fields as medical care, new materials, manufacturing, and finance. Toppan, the NICT, QunaSys, and ISARA will collaborate to combine their various accumulated technologies, expertise, and experience for development. Pilot testing of application software for implementation in wider society is scheduled to begin during fiscal 2022, with limited practical implementation targeted in 2025, and the launch of services planned for 2030.

Background

It has become increasingly important in recent years for businesses to be able to minimize damage to offices, plants, data centers, and other resources and enable the continuation or prompt restoration of core operations in the event of natural disasters, large-scale fires, terrorist attacks, and other emergencies. With the recent digital shift, it is also now essential that companies can safely store large volumes of important data and recover it in its entirety when necessary. However, there are technical limitations on the ability to ensure resilience against unforeseeable natural or man-made disasters in the future. This creates a need for ultra-long-term, high-security cloud technologies for the distributed and secure storage and complete recovery of information.

Cryptography that is currently widely used makes secure communication possible. However, with the practical application of quantum computing technologies expected to be seen around 2030, there is concern that it will be possible to decrypt highly-sensitive communications, such as electronic payments and digital application forms containing personal data. Uncrackable encryption technologies will therefore be required as society is faced with the challenge of bolstering security.

Details of the collaboration

The collaboration between the four organizations will aim to establish quantum secure cloud technology as infrastructure for data storage/transfer and post-quantum public key authentication. This will be based on system design, consideration of specifications, application of the latest quantum cryptography technologies, implementation of backup and data storage using secret sharing technology, and the development of digital signatures based on post-quantum public key cryptography.

In addition, as part of the Japanese government's Cross-ministerial Strategic Innovation Promotion Program (SIP), the NICT is working to establish international standards and is aiming to make proposals to such organizations as the ITU-T, ISO/IEC, and ETSI by fiscal 2022. These proposals cover such areas as network requirements, architecture, and security requirements as well as the evaluation and testing of key management and quantum cryptography modules.

"Toppan is proud to be able to undertake R&D on quantum computing for the creation of Society 5.0 with organizations whose activities are leading the world. For many years we have been involved in operations handling personal and sensitive information as well as security businesses focused on authentication and payment. With concern over existing cryptography technology and security being compromised in the near future, Toppan sees the implementation of new security technologies in society as a major responsibility. Quantum secure cloud technology is a concept for a practical system combining such security technologies as next-generation quantum cryptography and secret sharing. By combining the expertise of each company, we aim to make this a reality and contribute to safety and security in the age of quantum computing," said Hiroki Shibatani, Executive Officer of Toppan's DX Design Division.

"The NICT has been working on the development of quantum cryptography for more than 20 years. It is being used for state-level confidential communications and by financial and medical institutions, but is still at the stage of research. In the field of quantum cryptography, China is conducting testing on a far greater scale than other nations, and Japan is lagging behind in this respect. With this collaboration, we hope to establish a 'made-in-Japan' quality assurance platform for standardization and ensure that Japan takes the lead going forward. Society 5.0 will see the generation of highly sensitive personal data and high-value business information. It is vitally important that businesses and users are able to store, share, and use that information securely. I am confident that by making quantum secure cloud technology a reality with this collaboration and establishing the foundations to support Society 5.0, we will be able to help enhance Japan's competitiveness," said Masahide Sasaki, Distinguished Researcher, Advanced ICT Research Institute, NICT.

"With such developments as Google's achievement of quantum supremacy, there have been numerous breakthroughs in quantum computing in recent years, and we are getting closer to practical application. However, when it comes to the widespread application of a new technology, concerns also accompany expectations. While quantum computing is anticipated to increase the speed of scientific calculation for materials, there is also the possibility that today's RSA cryptosystems could be cracked. Because QunaSys handles highly sensitive data for new materials, we feel the need for quantum cryptography technologies that can protect that confidential information. We believe that the quantum secure cloud technology targeted by this collaboration will be essential in the quantum computing age. By leveraging that technology, we aim to create services for material development, an area in which the use of quantum computers is highly anticipated," said Tennin Yan, CEO, QunaSys.

"The quantum computing era is expected to begin within the next seven to 15 years, and there are indications that existing cryptographic technologies could be compromised. Work to standardize quantum-safe cryptography that is believed to be secure against attacks by quantum computers is therefore underway. It is important to note, however, that it will take time to migrate to quantum-safe cryptography. For example, the modernization of cryptography used by the U.S. Armed Forces, including initiatives to transition from RSA to ECC, remains incomplete after 20 years. It is too late to act once a threat has arisen, so it is essential to promptly formulate plans and start to implement measures now. Quantum secure cloud technology is something that can counteract those threats. We believe that if it can be incorporated into social infrastructure, then there is a large market for it. By leveraging ISARA's expertise in cryptography migration based on quantum-safe and crypto-agile technologies, we intend to explore the ideal vision for the quantum computing era and contribute to social change," said Atsushi Yamada, Vice President, Research & Development, ISARA Corporation.

19 The encryption war is on again, and this time government has a new strategy

by Steve Ranger

https://www.zdnet.com/article/the-encryption-war-is-on-again-and-this-time-government-has-a-new-strategy/

We could soon be in for a new round of the encryption wars, but this time governments are taking a different approach.

Seven governments from across the world have started a new campaign to try and persuade big tech companies to reduce the level of security they offer to customers using their services.

The seven – US, UK, Canada, Australia , New Zealand, India and Japan – are worried that the use of end-to-end encryption makes it impossible for tech companies to identify dangerous content like terrorist propaganda and attack planning, and makes it harder for police to investigate serious crimes and protect national security.

Their statement starts boldly: "We, the undersigned, support strong encryption", saying that it plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cybersecurity, and in repressive states protects journalists, human rights defenders and other vulnerable people.

Then, of course, comes the big caveat: "We urge industry to address our serious concerns where encryption is applied in a way that wholly precludes any legal access to content." The sort of end-to-end encryption that means messages can't be intercepted, or that a hard drive can never be read without the key, "pose significant challenges to public safety", the seven governments warn.

This of course is where things get trickier. These governments want tech companies to make it possible to act against illegal content and activity, but with no reduction to safety – something that tech companies insist is impossible.

"We challenge the assertion that public safety cannot be protected without compromising privacy or cybersecurity. We strongly believe that approaches protecting each of these important values are possible and strive to work with industry to collaborate on mutually agreeable solutions," the statement concludes.

Tech companies argue that end-to-end encryption protects users' privacy rights, and it to weaken it – by creating a so-called 'backdoor' that would allow the authorities to look at messages – would put all sorts of private communications at risk from hackers and force them to decide whether to hand over messages to oppressive regimes. End-to-end encryption makes the tech companies' lives easier, and also allows them to claim the moral high-ground when it comes to privacy.

So it there anything new in this? Governments have been half-heartedly trying to refight the cryptowars for years now, with little success – largely because they know that coming up with a fix for this is hard.

They know it's all but impossible to ban the use of end-to-end encryption. Sure, you could pass laws to ban it, and maybe block encrypted apps from local app stores if they used it, or make it illegal to posses them. But that's insanely hard to justify and even harder to enforce – even for states like Russia, which have tried to ban encrypted services.

And even if you did go for a ban, organised crime would simply get hold of encryption on the black market or from abroad, and would be just as well-protected as ever. But the average person on the street would be unable to access strong encryption, and would be more at risk of hacking as a result.

A policy that makes the average person less secure, while doing little to tackle the real problem, seems unlikely to gain much support. Imagine being the politician who has to explain to the country that their data has just been scooped up by a foreign power as a result.

The UK's GCHQ has come up with an idea called 'ghost protocol', which would add the government as a secret eavesdropper into every call. But although GCHQ's scheme has technical merit, if tech companies said 'yes' to one agency they would struggle to exclude others – that chat with your mates about what to watch on Netflix could quickly become crowded with spies from around the world.

That's because governments will inevitably over-reach and use such powers to increase their general surveillance. It's worth remembering that many of these tech companies introduced end-to-end encryption precisely because governments were cheerfully snooping on everyone's conversations in the first place. Many would say it's brazen of governments to now ask us to trust them again.

A new approach

So what's going on here? Adding two new countries – Japan and India – the statement suggests that more governments are getting worried, but the tone is slightly different now. Perhaps governments are trying a less direct approach this time, and hoping to put pressure on tech companies in a different way.

"I find it interesting that the rhetoric has softened slightly," says Professor Alan Woodward of the University of Surrey. "They are no longer saying 'do something or else' ".

What this note tries to do is put the ball firmly back in the tech companies' court, Woodward says, by implying that big tech is putting people at risk by not acceding to their demands – a potentially effective tactic in building a public consensus against the tech companies.

"It seems extraordinary that we're having this discussion yet again, but I think that the politicians feel they are gathering a head of steam with which to put pressure on the big tech companies," he says.

Even if police and intelligence agencies can't always get encrypted messages from tech companies, they certainly aren't without other powers. The UK recently passed legislation giving law enforcement wide-ranging powers to hack into computer systems in search of data.

So will governments find more success with their new softer approach? In the short term, probably not. End-to-end encryption creates real and tragic problems for police and the victims of crime, yet governments have not made a decent case for making us all less secure in response to those problems. Still, governments are increasingly conscious of the impact of big tech companies, and are increasingly willing to take them on. It may only take a few high-profile situations where strong encryption prevents a terrible crime from being stopped or investigated, for governments to think that public opinion can be shifted in their direction.

20 UK says Russia was preparing cyber-attacks against the Tokyo Olympics

by Catalin Cimpanu

https://www.zdnet.com/article/uk-says-russia-was-preparing-cyber-attacks-against-the-tokyo-olympics/

The UK government said today that Russian hackers were preparing cyber-attacks against the organizers of the Tokyo Olympics and Paralympic Games that were set to take place this summer in Japan before they were postponed to next year due to the ongoing COVID-19 pandemic.

Russian activity involved reconnaissance operations, according to a press release from the UK National Cyber Security Centre (NCSC).

Targets included the Games' organizers, logistics services, and sponsors, the UK government said in a separate press release.

“The GRU's actions against the Olympic and Paralympic Games are cynical and reckless,” said UK Foreign Secretary Dominic Raab.

“We condemn them in the strongest possible terms.”

UK authorities believe Russian hackers intended to sabotage the Olympic Games, similar to the cyber-attacks they carried out against the organizers of the 2018 Winter Olympic and Paralympic Games in Pyeongchang, South Korea.

In February 2018, Russian hackers deployed the **OlympicDestroyer** malware that crippled web servers during the opening ceremony of the 2018 Winter Olympics.

The attacks were carried out because the International Olympic Committee had banned Russian athletes from participating at the event under the Russian flag, citing a state-sponsored doping program.

The same ban, originally imposed for the Rio 2016 Summer Olympics, has also been extended to the Tokyo Olympics this year, with Russian athletes being banned from competing under the Russian flag again.

Now, UK officials say that Russia appears to have been preparing similar attacks to sabotage the 2020 Olympics as well.

UK officials said that responsible for these planned attacks was a Russian hacking group known as Sandworm, the same group behind the OlympicDestroyer destructive attacks at the Pyeongchang Olympics.

SANDWORM HACKERS CHARGED IN THE US

The UK government's statement coincided with the announcement of formal charges against six Sandworm members by the US Department of Justice earlier today.

US officials charged Sandworm hackers for orchestrating not only the OlympicDestroyer attacks at the 2018 Pyeongchang Olympics but also a series of many other attacks, such as:

- attempts to sabotage Ukraine's power grid in 2015 and 2016 with the BlackEnergy and Industroyer malware
- attempts to sabotage Ukrainian government networks with the KillDisk disk-wiping malware
- creating the NotPetya ransomware that caused a global outbreak in June 2017
- interfering in the French 2017 elections
- arranging cyber-attacks against the organizations investigating the Novichok poisonings in the UK

- mass-defacing thousands of Georgian sites in 2019

US officials blamed these attacks on Sandworm, a hacker group it said was composed of members of Unit 74455 of the Russian Main Intelligence Directorate (GRU), a military intelligence agency part of the Russian Army.

In its press release today, the UK government issued formal confirmation of the accusations put forward in the US indictments but also exposed and raised a sign of alarm about Sandworm's impending attacks on Tokyo 2020 Olympics organizers.

21 This new malware uses remote overlay attacks to hijack your bank account

by Charlie Osborne

https://www.zdnet.com/article/this-new-malware-uses-remote-overlay-attacks-to-hijack-your-bank-account/

Researchers have uncovered a new form of malware using remote overlay attacks to strike Brazilian bank account holders.

The new malware variant, dubbed **Vizom** by IBM, is being utilized in an active campaign across Brazil designed to compromise bank accounts via online financial services.

On Tuesday, IBM security researchers Chen Nahman, Ofir Ozer, and Limor Kessem said the malware uses interesting tactics to stay hidden and to compromise user devices in real-time – namely, remote overlay techniques and DLL hijacking.

Vizom spreads through spam-based phishing campaigns and disguises itself as popular videoconferencing software, tools that have become crucial to businesses and social events due to the coronavirus pandemic.

Once the malware has landed on a vulnerable Windows PC, Vizom will first strike the AppData directory to begin the infection chain. By harnessing DLL hijacking, the malware will attempt to force the loading of malicious DLLs by naming its own Delphi-based variants with names expected by the legitimate software in their directories.

By hijacking a system's "inherent logic," IBM says the operating system is tricked into loading Vizom malware as a child process of a legitimate videoconferencing file. The DLL is named Cmmlib.dll, a file associated with Zoom.

"To make sure that the malicious code is executed from "Cmmlib.dll," the malware's author copied the real export list of that legitimate DLL but made sure to modify it and have all the functions direct to the same address – the malicious code's address space," the researchers say.

A dropper will then launch *zTscoder.exe* via command prompt and a second payload, a Remote Access Trojan (RAT), is extracted from a remote server – with the same hijacking trick performed on the Vivaldi Internet browser.

To establish persistence, browser shortcuts are tampered with and no matter what browser a user attempts to run, the malicious Vivaldi/Vizom code will run in the background.

The malware will then quietly wait for any indication that an online banking service is being accessed.

If a webpage's title name matches Vizom's target list, operators are alerted and can connect remotely to the compromised PC.

As Vizom has already deployed RAT capabilities, attackers can take over a compromised session and overlay content to trick victims into submitting access and account credentials for their bank accounts.

Remote control capabilities also abuse Windows API functions, such as moving a mouse cursor, initiating keyboard input, and emulating clicks. Vizom can also grab screenshots through Windows print and magnifier functions.

In order to create convincing overlays, the malware generates HTML files and then loads them in Vivaldi in application mode. A keylogger is then launched, with input encrypted, packaged, and whisked away to the attacker's command-and-control (C2) server.

"The remote overlay malware class has gained tremendous momentum in the Latin American cybercrime arena through the past decade making it the top offender in the region," IBM says. "At this time, Vizom focuses on large Brazilian banks, however, the same tactics are known to be used against users across South America and has already been observed targeting banks in Europe as well."

22 Japanese consortium for post-quantum secure cloud

by Nick Flaherty

https://www.eenewseurope.com/news/japanese-consortium-post-quantum-secure-cloud

The threat of quantum computing is driving a consortium of Toppan Printing, NICT, QunaSys and Isara in Japan to develop a post-quantum secure cloud service Four Japanese organisations have formed a consortium to develop post-quantum cloud technology that is secure against quantum computer attacks.

Toppan Printing, the National Institute of Information and Communications Technology (NICT), quantum algorithm specialist QunaSys and cybersecurity firm Isara will develop secure processing, communication, storage, and use of data.

The move is not just a response to the roll out of US quantum computers from companies such as D-Wave, Rigetti and IBM with quantum computing services already available on Amazon Web Sevices, but also the challenge from China. "In the field of quantum cryptography, China is conducting testing on a far greater scale than other nations, and Japan is lagging behind in this respect," said Masahide Sasaki, Distinguished Researcher at the Advanced ICT Research Institute at NICT. European standards group ETSI has also published guidance on post-quantum security,

- ETSI guidance for a quantum-safe world
- Quantum computing available via Amazon Web Services

Post-quantum encryption technologies will be important for the collection, analysis, processing, and use of highly sensitive personal and corporate information accumulated in such fields as medical care, new materials, manufacturing, and finance in public and private cloud infrastructure.

Pilot testing of application software is scheduled to begin during 2022, with limited practical implementation targeted in 2025, and the launch of services planned for 2030. The timing is in part determined by the development of encrpyption standards for post-quantum encryption in the next two years and the asssociated hardware standards. The first quantum-secure point to point networks are already rolling out.

The group sees practical application of quantum computing technologies around 2030, making it possible to decrypt highly-sensitive communications such as electronic payments and digital application forms containing personal data. Post-quantum encryption technologies will therefore be required as society is faced with the challenge of bolstering security.

The collaboration aims to establish quantum-secure cloud technology as infrastructure for data storage/transfer and post-quantum public key authentication. This will be based on system design, consideration of specifications, application of the latest quantum cryptography technologies, implementation of backup and data storage using secret sharing technology, and the development of digital signatures based on post-quantum public key cryptography.

NICT is also working to establish international standards and is aiming to make proposals to such organizations as the ITU-T, ISO/IEC, and ETSI by fiscal 2022. These proposals cover such areas as network requirements, architecture, and security requirements as well as the evaluation and testing of key management and quantum cryptography modules.

Toppan Printing is contributing its expertise from smartcard technology, while QunaSys has built up a range of quantum computing technologies through the development of quantum computer algorithms and Qamuy, a piece of quantum chemistry calculation software that makes use of quantum computers. QunaSys will drive the provision of material development services using the quantum secure cloud technology and also contribute its user expertise.

“Toppan is proud to be able to undertake R&D on quantum computing for the creation of Society 5.0 with organizations whose activities are leading the world. For many years we have been involved in operations handling personal and sensitive information as well as security businesses focused on authentication and payment. With concern over existing cryptography technology and security being compromised in the near future, Toppan sees the implementation of new security technologies in society as a major responsibility. Quantum secure cloud technology is a concept for a practical system combining such security technologies as next-generation quantum cryptography and secret sharing. By combining the expertise of each company, we aim to make this a reality and contribute to safety and security in the age of quantum computing,” said Hiroki Shibatani, Executive Officer of Toppan’s DX Design Division.

“The NICT has been working on the development of quantum cryptography for more than 20 years. It is being used for state-level confidential communications and by financial and medical institutions, but is still at the stage of research. With this collaboration, we hope to establish a ‘made-in-Japan’ quality assurance platform for standardization and ensure that Japan takes the lead going forward. Society 5.0 will see the generation of highly sensitive personal data and high-value business information. It is vitally important that businesses and users are able to store, share, and use that information securely. I am confident that by making quantum secure cloud technology a reality with this collaboration and establishing the foundations to support Society 5.0, we will be able to help enhance Japan’s competitiveness,” said Sasaki at NICT.

“With such developments as Google’s achievement of quantum supremacy, there have been numerous breakthroughs in quantum computing in recent years, and we are getting closer to practical application. However, when it comes to the widespread application of a new technology, concerns also accompany expectations. While quantum computing is anticipated to increase the speed of scientific calculation for materials, there is also the possibility that today’s RSA cryptosystems could be cracked. Because QunaSys handles highly sensitive data for new materials, we feel the need for quantum cryptography technologies that can protect that confidential information. We believe that the quantum secure cloud technology targeted by this collaboration will be essential in the quantum computing age. By leveraging that technology, we aim to create services for material development, an area in which the use of quantum computers is highly anticipated," said Tennin Yan, CEO of QunaSys.

"The quantum computing era is expected to begin within the next seven to 15 years, and there are indications that existing cryptographic technologies could be compromised. Work to standardize quantum-safe cryptography that is believed to be secure against attacks by quantum computers is therefore underway. It is important to note, however, that it will take time to migrate to quantum-safe cryptography. For example, the modernization of cryptography used by the U.S. Armed Forces, including initiatives to transition from RSA to ECC, remains incomplete after 20 years. It is too late to act once a threat has arisen, so it is essential to promptly formulate plans and start to implement measures now. Quantum secure cloud technology is something that can counteract those threats. We believe that if it can be incorporated into social infrastructure, then there is a large market for it. By leveraging ISARA's expertise in cryptography migration based on quantum-safe and crypto-agile technologies, we intend to explore the ideal vision for the quantum computing era and contribute to social change," said Atsushi Yamada, Vice President, Research & Development, ISARA Corporation.

18 Oct 2020

23 Google stops biggest-ever DDoS cyber attack to date

by IANS

https://cio.economictimes.indiatimes.com/news/digital-security/google-stops-biggest-ever-ddos-cyber-attack-to-date/78728398

The cyber security threats such as distributed denial-of-service (DDoS) are growing exponentially, disrupting businesses of all sizes globally, leading to outages and loss of user trust, Google has said.

The tech giant revealed that its infrastructure absorbed a massive 2.5Tbps DDoS in September 2017, the highest-bandwidth attack reported to date which was the culmination of a six-month campaign that utilised multiple methods of attack.

"Despite simultaneously targeting thousands of our IPs, presumably in hopes of slipping past automated defenses, the attack had no impact," Google said in a statement on Friday.

The attacker used several networks to spoof 167 Mbps (millions of packets per second) to 180,000 exposed CLDAP, DNS, and SMTP servers, which would then send large responses to Google.

"This demonstrates the volumes a well-resourced attacker can achieve: This was four times larger than the record-breaking 623 Gbps attack from the Mirai botnet a year earlier. It remains the highest-bandwidth attack reported to date, leading to reduced confidence in the extrapolation," the company informed.

With a DDoS attack, an adversary hopes to disrupt their victim's service with a flood of useless traffic.

While this attack doesn't expose user data and doesn't lead to a compromise, it can result in an outage and loss of user trust if not quickly mitigated.

Attackers are constantly developing new techniques to disrupt systems.

"Some attacks may not even focus on a specific target, but instead attack every IP in a network. Multiplying the dozens of attack types by the diversity of infrastructure that must be defended leads to endless possibilities," Google said.

The company said the main task is to determine the capacity needed to withstand the largest DDoS attacks for each key metric.

"While we can estimate the expected size of future attacks, we need to be prepared for the unexpected, and thus we over-provision our defenses accordingly".

24 China advances quantum sci-tech, early blueprint to 'counter tech blockade'

https://www.globaltimes.cn/content/1203855.shtml

After a group study session of the Political Bureau of the Communist Party of China Central Committee emphasized the importance and urgency of advancing the development of quantum science and technology, scientists lauded the favourable policies while observers noted it shows China's vision in science in an uncertain world.

President Xi Jinping stressed the importance of strengthening strategic planning and systematic layout for the development of quantum science and technology at the session held on Friday.

Xi emphasized the need to strengthen top-level design and forward-looking layout of the area, improve the policy support systems, and speed up breakthroughs in basic research.

He also stressed speeding up fostering talent in the field of quantum science and technology by training a number of high-level talent, establishing a special training plan suitable for the development of quantum science and technology and building a systematic and high-level training platform for talent in the area.

Quantum information science has become a new area of world competition. In the UK, metropolitan quantum networks have been built by the Quantum Communications Hub in Cambridge and Bristol, connected by a long-distance link via London. The EU has documentation to jointly develop high performance computing, including quantum computing, in the next decade. The US has a National Quantum Initiative involving 16 different federal agencies and offices and its technology giants are taking lead in quantum computing.

China listed **quantum communication** in its 13th Five-Year Plan (2016-20). China's scientific and technological workers have made great efforts to catch up in quantum science and technology and made a number of significant innovations with international influence.

China launched the Quantum Experiments at Space Scale program, better known as Micius in 2016 and has conducted multiple space-ground quantum communication experiments.

Chinese scientists are also cooperating with their Austrian counterparts in developing quantum communication technology.

Quantum communication is commonly used to protect information channels by means of quantum cryptography. QuantumCTek Co, China's biggest listed company in the field is worth 24 billion yuan ($3.58 billion), but the field overall faces the challenge of high costs in commercial use.

Guo Guoping, a key member of the research and development (R&D) team and a professor at the Hefei-based University of Science and Technology of China, told the Global Times that China takes a lead in quantum communication but lags three to five years behind in quantum computing.

The gap is not only in scientific research, but also in simulation and real application of quantum computing, Guo said.

US companies like Google, IBM and Microsoft are the industry giants while Chinese companies like Alibaba and Baidu are actively catching up.

China had nearly twice as many patent filings as the US for quantum technology overall in 2018, a category that includes communications and cryptology devices, according to market research firm Patinformatics. The US leads the world in patents relating to quantum computers, the hottest segment of quantum science and technology, media reported.

Chinese researchers are also planning to take a quantum leap in computing, and even to compete with Google's Sycamore which is enabled by a 53-qubit superconductivity system with 99.4% fidelity, in 10 years.

Zhu Xiaobo, a professor with the Shanghai-based Institute of Advanced Studies affiliated with the University of Science and Technology of China said in August that a 60-qubit superconductivity quantum computing system with 99.5% fidelity could be achieved this year, and in 10 years, the system could evolve into a million-qubit level with a 99.8% fidelity, equivalent to, if not better than, its Google counterpart.

Google announced a breakthrough in October 2019. Using the company's state-of-the-art quantum computer, called Sycamore, Google claimed "quantum supremacy" over the most powerful supercomputers in the world by solving problems considered virtually impossible for normal machines.

Zhu hopes that in 10-15 years, quantum computers can be used to solve real problems in the field of cryptology, rather than being used only to demonstrate their computing capabilities, which is the case for current models.

Observers said this new blueprint in a pioneering area like quantum technology shows China's vision in basic science and key technologies, which is of more importance when uncertainties in global politics could threaten development and application of technologies.

China has learned its lesson from the chip industry, and an early layout for quantum technology will prevent that from happening again, they said.

As introducing talented professionals from overseas has become less possible, it is important and urgent to train young people, Li Chuanfeng, executive deputy director of the Chinese Academy of Sciences' Key Laboratory of Quantum Information, told the Global Times on Sunday.

Some insiders also discussed whether quantum information science should become a first-class discipline instead of a sub-discipline of physics in China as it is now. Such a change means that universities could directly enroll young people with an interest in the field and foster them to become quantum information scientists.

At the group study session, Xi called for efforts to make breakthroughs in key core technologies, ensure the safety of industrial and supply chains, and enhance China's ability of responding to international risks and challenges with science and technology.

At practical level, Guo suggested that research funds should not only go to universities and major scientific institutes but also be used as leverage to support companies in quantum applications. Such policies will help address the problem of industry-research cooperation as companies are by nature user-oriented, he said.

It is also timely to reform the evaluation system as quantum computing should not focus too much on theoretical studies and publishing papers. The industry requires a broader horizon for real application and what research can bring about, he said.

25 Toshiba targets $3 billion revenue in quantum cryptography by 2030

by Makiko Yamazaki

https://in.reuters.com/article/us-toshiba-cyber/toshiba-targets-3-billion-revenue-in-quantum-cryptography-by-2030-idUSKBN2730KW

Toshiba Corp 6502.T said on Monday it aims to generate $3 billion in revenue from its advanced cryptographic technology for data protection by 2030, as the Japanese sprawling conglomerate scrambles to find future growth drivers.

The cyber security technology, called quantum key distribution (QKD), leverages the nature of quantum physics to provide two remote parties with cryptographic keys that are immune to cyberattacks driven by quantum computers.

Toshiba expects the global QKD market to grow to $12 billion in 10 years with the advance of quantum computers, whose massive computational power could easily decipher conventional math-based cryptographic keys commonly used in finance, defence and health care.

The company is hoping to tap global demand for advanced cryptographic technologies as cyber security has come to the forefront of national defence. China is aggressively expanding network infrastructure for QKD, including quantum satellites that relay quantum signals.

The company said it has teamed up with Verizon Communications Inc VZ.N in the United States and BT Group BT.L in Britain in pilot QKD projects, and is in talks with another telecommunications carrier in South Korea.

Since a crisis stemming from the bankruptcy of the U.S. nuclear power business in 2017, Toshiba has conducted a series of restructuring steps, including the sale of its laptop and television set businesses.

It is now focusing on public infrastructure businesses that are resilient to a global economic slump driven by the coronavirus outbreak.

17 Oct 2020

26 Design Your Own Superconducting Qubits with IBM's Qiskit Metal

https://quantumcomputingreport.com/design-your-own-superconducting-qubits-with-ibms-qiskit-metal/

IBM is releasing an open source computer aided design (CAD) program called Qiskit Metal that will allow a user to layout and analysis a superconducting qubit. The program will include a library of elements such as transmon qubits and coplanar resonators and includes a graphical interface that will allow a user to lay them out connect them and also their shape as desired. It also includes modelling functions that will allow a user to predict such characteristics as qubit frequencies, anharmonicities, couplings, and dissipation and include the ability to interface with other electromagnetic analysis tools to simulate a design. The resulting design can then be output in a semiconductor industry standard GDSII layout file for creation of a mask and fabrication at a semiconductor fab.

The program is intended for quantum hardware designers (including potentially IBM's superconducting competitors). It is unique among all the publicly available quantum software packages we are aware of because it is focused on the physical design and analysis of the qubits themselves. IBM will initiate an early access program in November which will extend through March 2021.

27 Ransomware attack hits Haldiram's

by Shikha Salaria

https://ciso.economictimes.indiatimes.com/news/ransomware-attack-hits-haldirams/78713883

Snacks manufacturer Haldiram's faced a ransomware attack on its servers by hackers who allegedly encrypted all their files, data, applications and systems and demanded a ransom of US $7,50,000 for access. While a complaint was submitted to the cyber cell on July 17 this year, according to officials, an FIR was lodged in the case in October 14.

According to the FIR lodged at Sector 58 police station, on July 13 around 1.30 am, the IT department of Haldiram's got to know that a few orders had been held up as there was a problem with the server.

"That on receipt of the information, senior manager (IT) Ashok Kumar Mohanty informed Aziz Khan, DGM (IT) to resolve the issue. However, on accessing the servers of the company, Aziz Khan, found out that all the servers of the company had been hacked and hit by a cyber-attack/malware popularly called as a Ransomware Attack," the FIR read.

16 Oct 2020

28 Five cryptologic giants inducted into the NSA/CSS Cryptologic Hall of Honor

https://www.nsa.gov/news-features/press-room/Article/2384364/five-cryptologic-giants-inducted-into-the-nsacss-cryptologic-hall-of-honor/

The National Security Agency inducted five new cryptologic figures into the Cryptologic Hall of Honor at the National Security Agency, Oct. 16.

The new members of the Cryptologic Hall of Honor are:

- **Mr. George Cotter** – For over half a century, Mr. Cotter fostered the adoption of advanced technology in support of NSA's mission. He led the agency in adopting high performance computers and adapting them to the mission, and was founding director of the National Computer Security Center. His influence on computerization extended to the entire intelligence community and foreign partners.

- **Dr. Whitfield Diffie** – Dr. Diffie's innovative work in computer and internet security has enhanced the security of all users – government and civilian alike. His research at university facilities and private laboratories led the way in computer security theory and in practical applications.

- **Dr. David Kahn** – Dr. Kahn pioneered the study of cryptologic history as an academic field and helped practitioners understand their heritage. His popular writings on cryptology and its history inspired hundreds of individuals to study cryptology and to seek employment at NSA. In addition to his books and articles, Dr. Kahn's public appearances have helped improve the image of government cryptology to the nation at large.
- **Ms. Barbara McNamara** – Throughout the middle and end of the Cold War, Ms. McNamara's expert leadership resulted in increased intelligence production on critical targets. Her deft touch was important in improving NSA's relationship within the U.S. Intelligence community and with foreign partners. Ms. McNamara's experience enabled her to shape an operational component at NSA for the post-Cold War era.
- **Mr. Lester Myers** – Mr. Myers' superior language skills and deep area knowledge were crucial to successful fulfillment of NSA's missions in many crises from the 1970's and into the 21st century. In addition to his expert use of language in operational situations, Mr. Myers developed advanced reference materials and mentored the next generation of military and civilian linguists.

29 What if We Had a Computer-Aided Design Program for Quantum Computers?

by Qiskit

https://medium.com/qiskit/what-if-we-had-a-computer-aided-design-program-for-quantum-computers-4cb88bd1ddea

There's no doubt about it: building quantum computers is hard, and we wish it was easier.

Designing quantum devices is the bedrock of the quantum computing world, and yet, this is an arduous, multi-step process more complex than the design workflow of conventional chips. The quanutm hardware designers have to work across several normally-disconnected worlds, developing and benchmarking computer chips that incorporate superconducting metal parts and follow the rules of quantum electrodynamics (QED). This requires a suite of development and analysis techniques without a classical analog. But if we want to actually build and use these amazing devices, we'll need to find a way to make this process easier.

On the surface, designing a quantum chip should be a lot like designing any other integrated circuit. But a typical integrated circuit goes through a design flow process that's had decades worth of tuning. As chips have scaled up in transistor count in step with Moore's law, design tools have matured in kind, becoming automated. Today, a sequence of programs allow chip designers to think in a modular way about integrated circuits with billions of transistors, in a process that rather seamlessly creates and tests designs, then moves them to the fabrication stage.

Quantum computers are not like today's computer microprocessors, though. Quantum bits are much larger than transistors, and require more complex superconducting circuitry. Computer-aided electronic design automation software covers only some parts of this intricate fabrication process, and using these software packages to design a quantum computer comes with a high barrier to entry.

If we want quantum computers to one day scale and mature in the same way that classical computers have, we'll need to begin thinking about quantum electronic design automation (EDA) tools in kind. Meanwhile, within our own community, we want to accelerate and lower the barrier to innovation on quantum devices. The IBM Quantum team is therefore beginning to think about what EDA might look like for a quantum processor, and hopes that the community will begin thinking about it, too. Today at the IEEE Quantum Week Conference, the team discussed their vision for this first-of-its-kind project. Led by quantum physicist Zlatko Minev and developed with other IBM Quantum team members, this project is meant for those interested in quantum hardware design: a suite of design automation tools that can be used to devise and analyze superconducting devices, with a focus on being able to integrate the best tools into a quantum hardware designer's workflow. We've code-named the project Qiskit Metal.

We hope that as a community, we might make the process of quantization – bridging the gap between pieces of a superconducting metal on a quantum chip with the computational mathematics of Hamiltonians and Hilbert spaces – available to anyone with a curious mind and a laptop. We want to make quantum device design a streamlined process that automates the laborious tasks as it does with conventional electronic device design. We are writing software with built-in best practices and cutting-edge quantum analysis techniques, all this while seamlessly leveraging the power of conventional EDA tools. The goal of Qiskit Metal is to allow for easy quantum hardware modeling with reduction of design-related errors plus increased speed.

Internally, we have started to test the program's analysis techniques, and in an upcoming publication, Zlatko Minev, Thomas McConkey & Jay Gambetta will share some early results that demonstrate percent-level agreement between design analysis and experimental hardware. This project is an exciting work in progress in its early development stages, and might not remain "Qiskit Metal" for long. We hope that we can spur the community to begin thinking about design automation for quantum computers, and draw in experts in the field of classical computing to help. Therefore, it's crucial that we keep this project open source so that engineers around the world can help solve this to-be pressing problem.

We are thrilled to ask the community to work closely with us in developing Qiskit Metal through an early-access program, starting in November.

30 Research team discovers uniquely quantum effect in erasing information

by Trinity College Dublin

https://phys.org/news/2020-10-team-uniquely-quantum-effect-erasing.html

Researchers from Trinity have discovered a uniquely quantum effect in erasing information that may have significant implications for the design of quantum computing chips. Their surprising discovery brings back to life the paradoxical "Maxwell's demon," which has tormented physicists for over 150 years.

The thermodynamics of computation was brought to the fore in 1961 when Rolf Landauer, then at IBM, discovered a relationship between the dissipation of heat and logically irreversible operations. Landauer is known for the mantra "Information is Physical," which reminds us that information is not abstract and is encoded on physical hardware.

The "bit" is the currency of information (it can be either zero or one) and Landauer discovered that when a bit is erased there is a minimum amount of heat released. This is known as Landauer's bound and is the definitive link between information theory and thermodynamics.

Professor John Goold's QuSys group at Trinity is analyzing this topic with quantum computing in mind, where a quantum bit (a qubit, which can be zero and one at the same time) is erased.

In just-published work in the journal, Physical Review Letters, the group discovered that the quantum nature of the information to be erased can lead to large deviations in the heat dissipation, which is not present in conventional bit erasure.

Thermodynamics and Maxwell's demon

One hundred years previous to Landauer's discovery people like Viennese scientist, Ludwig Boltzmann, and Scottish physicist, James Clerk Maxwell, were formulating the kinetic theory of gases, reviving an old idea of the ancient Greeks by thinking about matter being made of atoms and deriving macroscopic thermodynamics from microscopic dynamics.

Professor Goold says: "Statistical mechanics tells us that things like pressure and temperature, and even the laws of thermodynamics themselves, can be understood by the average behavior of the atomic constituents of matter. The second law of thermodynamics concerns something called entropy which, in a nutshell, is a measure of the disorder in a process. The second law tells us that in the absence of external intervention, all processes in the universe tend, on average, to increase their entropy and reach a state known as thermal equilibrium.

"It tells us that, when mixed, two gases at different temperatures will reach a new state of equilibrium at the average temperature of the two. It is the ultimate law in the sense that every dynamical system is subject to it. There is no escape: all things will reach equilibrium, even you."

However, the founding fathers of statistical mechanics were trying to pick holes in the second law right from the beginning of the kinetic theory. Consider again the example of a gas in equilibrium: Maxwell imagined a hypothetical "neat-fingered" being with the ability to track and sort particles in a gas based on their speed.

Maxwell's demon, as the being became known, could quickly open and shut a trap door in a box containing a gas, and let hot particles through to one side of the box but restrict cold ones to the other. This scenario seems to contradict the second law of thermodynamics as the overall entropy appears to decrease and perhaps physics' most famous paradox was born.

But what about Landauer's discovery about the heat-dissipated cost of erasing information? Well, it took another 20 years until that was fully appreciated, the paradox solved, and Maxwell's demon finally exorcised.

Landauer's work inspired Charlie Bennett – also at IBM – to investigate the idea of reversible computing. In one982 Bennett argued that the demon must have a memory, and that it is not the measurement but the erasure of the information in the demon's memory which is the act that restores the second law in the paradox. And, as a result, computation thermodynamics was born.

New findings

Now, 40 years on, this is where the new work led by Professor Goold's group comes to the fore, with the spotlight on quantum computation thermodynamics.

In the recent paper, published with collaborator Harry Miller at the University of Manchester and two postdoctoral fellows in the QuSys Group at Trinity, Mark Mitchison and Giacomo Guarnieri, the team studied very carefully an experimentally realistic erasure process that allows for quantum superposition (the qubit can be in state zero and one at same time).

Professor Goold explains: “In reality, computers function well away from Landauer’s bound for heat dissipation because they are not perfect systems. However, it is still important to think about the bound because as the miniaturization of computing components continues, that bound becomes ever closer, and it is becoming more relevant for quantum computing machines. What is amazing is that with technology these days you can really study erasure approaching that limit.

“We asked, ‘What difference does this distinctly quantum feature make for the erasure protocol?’ And the answer was something we did not expect. We found that even in an ideal erasure protocol – due to quantum superposition – you get very rare events which dissipate heat far greater than the Landauer limit.

“In the paper, we prove mathematically that these events exist and are a uniquely quantum feature. This is a highly unusual finding that could be really important for heat management on future quantum chips – although there is much more work to be done, in particular in analyzing faster operations and the thermodynamics of other gate implementations.

“Even in 2020, Maxwell’s demon continues to pose fundamental questions about the laws of nature.”

15 Oct 2020

31 Could Schrödinger’s cat exist in real life? Our research may soon provide the answer

by Stefan Forstner

https://phys.org/news/2020-10-schrdinger-cat-real-life.html

Have you ever been in more than one place at the same time? If you’re much bigger than an atom, the answer will be no.

But atoms and particles are governed by the rules of quantum mechanics, in which several different possible situations can coexist at once.

Quantum systems are ruled by what’s called a “wave function”: a mathematical object that describes the probabilities of these different possible situations.

And these different possibilities can coexist in the wave function as what is called a “superposition” of different states. For example, a particle existing in several different places at once is what we call “spatial superposition”.

It’s only when a measurement is carried out that the wave function “collapses” and the system ends up in one definite state.

Generally, quantum mechanics applies to the tiny world of atoms and particles. The jury is still out on what it means for large-scale objects.

In our research, published today in Optica, we propose an experiment that may resolve this thorny question once and for all.

Erwin Schrödinger’s cat

In the 1930s, Austrian physicist Erwin Schrödinger came up with his famous thought experiment about a cat in a box which, according to quantum mechanics, could be alive and dead at the same time.

In it, a cat is placed in a sealed box in which a random quantum event has a 50-50 chance of killing it. Until the box is opened and the cat is observed, the cat is both dead and alive at the same time.

In other words, the cat exists as a wave function (with multiple possibilities) before it's observed. When it's observed, it becomes a definite object.

After much debate, the scientific community at the time reached a consensus with the "Copenhagen interpretation". This basically says quantum mechanics can only apply to atoms and molecules, but can't describe much larger objects.

Turns out they were wrong.

In the past two decades or so, physicists have created quantum states in objects made of trillions of atoms – large enough to be seen with the naked eye. Although, this has not yet included spatial superposition.

How does a wave function become real?

But how does the wave function become a "real" object?

This is what physicists call the "quantum measurement problem". It has puzzled scientists and philosophers for about a century.

If there is a mechanism that removes the potential for quantum superposition from large-scale objects, it would require somehow "disturbing" the wave function – and this would create heat.

If such heat is found, this implies large-scale quantum superposition is impossible. If such heat is ruled out, then it's likely nature doesn't mind "being quantum" at any size.

If the latter is the case, with advancing technology we could put large objects, maybe even sentient beings, into quantum states.

Physicists don't know what a mechanism preventing large-scale quantum superpositions would look like. According to some, it's an unknown cosmological field. Others suspect gravity could have something to do with it.

This year's Nobel Prize winner for physics, Roger Penrose, thinks it could be a consequence of living beings' consciousness.

Chasing miniscule movements

Over the past decade or so, physicists have been feverishly seeking a trace amount of heat which would indicate a disturbance in the wave function.

To find this out, we'd need a method that can suppress (as perfectly as is possible) all other sources of "excess" heat that may get in the way of an accurate measurement.

We would also need to keep an effect called quantum "backaction" in check, in which the act of observing itself creates heat.

In our research, we've formulated such an experiment, which could reveal whether spatial superposition is be possible for large-scale objects. The best experiments thus far have not been able to achieve this.

Finding the answer with tiny beams that vibrate

Our experiment would use resonators at much higher frequencies than have been used. This would remove the issue of any heat from the fridge itself.

As was the case in previous experiments, we would need to use a fridge at 0.01 degrees kelvin above absolute zero. (Absoloute zero is the lowest temperature theoretically possible).

With this combination of very low temperatures and very high frequencies, vibrations in the resonators undergo a process called “Bose condensation”.

You can picture this as the resonator becoming so solidly frozen that heat from the fridge can’t wiggle it, not even a bit.

We would also use a different measurement strategy that doesn’t look at the resonator’s movement at all, but rather the amount of energy it has. This method would strongly suppress backaction heat, too.

But how would we do this?

Single particles of light would enter the resonator and bounce back and forth a few million times, absorbing any excess energy. They would eventually leave the resonator, carrying the excess energy away.

By measuring the energy of the light particles coming out, we could determine if there was heat in the resonator.

If heat was present, this would indicate an unknown source (which we didn’t control for) had disturbed the wave function. And this would mean it’s impossible for superposition to happen at a large scale.

Is everything quantum?

The experiment we propose is challenging. It’s not the kind of thing you can casually set up on a Sunday afternoon. It may take years of development, millions of dollars and a whole bunch of skilled experimental physicists.

Nonetheless, it could answer one of the most fascinating questions about our reality: is everything quantum? And so, we certainly think it’s worth the effort.

As for putting a human, or cat, into quantum superposition – there’s really no way for us to know how this would effect that being.

Luckily, this is a question we don’t have to think about, for now.

14 Oct 2020

32 Zoom to start first phase of E2E encryption rollout next week

by Natasha Lomas

https://techcrunch.com/2020/10/14/zoom-to-start-first-phase-of-e2e-encryption-rollout-next-week/?guccounter=1

Zoom will begin rolling out end-to-end encryption to users of its videoconferencing platform from next week, it said today.

The platform, whose fortunes have been supercharged by the pandemic-driven boom in remote working and socializing this year, has been working on rebooting its battered reputation in the areas of security and privacy since April – after it was called out on misleading marketing claims of having E2E encryption (when it did not). E2E is now finally on its way though.

“We’re excited to announce that starting next week, Zoom’s end-to-end encryption (E2EE) offering will be available as a technical preview, which means we’re proactively soliciting feedback from users for the first 30 days,” it writes in a blog post. “Zoom users – free and paid – around the world can host up to 200 participants in an E2EE meeting on Zoom, providing increased privacy and security for your Zoom sessions.”

Zoom acquired Keybase in May, saying then that it was aiming to develop “the most broadly used enterprise end-to-end encryption offering”.

However, initially, CEO Eric Yuan said this level of encryption would be reserved for fee-paying users only. But after facing a storm of criticism the company enacted a swift U-turn – saying in June that all users would be provided with the highest level of security, regardless of whether they are paying to use its service or not.

Zoom confirmed today that Free/Basics users who want to get access to E2EE will need to participate in a one-time verification process – in which it will ask them to provide additional pieces of information, such as verifying a phone number via text message – saying it’s implementing this to try to reduce “mass creation of abusive accounts”.

“We are confident that by implementing risk-based authentication, in combination with our current mix of tools – including our work with human rights and children’s safety organizations and our users’ ability to lock down a meeting, report abuse, and a myriad of other features made available as part of our security icon – we can continue to enhance the safety of our users,” it writes.

Next week’s roll out of a technical preview is phase 1 of a four-stage process to bring E2E encryption to the platform.

This means there are some limitations – including on the features that are available in E2EE Zoom meetings (you won’t have access to join before host, cloud recording, streaming, live transcription, Breakout Rooms, polling, 1:1 private chat, and meeting reactions); and on the clients that can be used to join meetings (for phase 1 all E2EE meeting participants must join from the Zoom desktop client, mobile app, or Zoom Rooms).

The next phase of the E2EE rollout – which will include “better identity management and E2EE SSO integration”, per Zoom’s blog – is “tentatively” slated for 2021.

From next week, customers wanting to check out the technical preview must enable E2EE meetings at the account level and opt-in to E2EE on a per-meeting basis.

All meeting participants must have the E2EE setting enabled in order to join an E2EE meeting. Hosts can enable the setting for E2EE at the account, group, and user level and can be locked at the account or group level, Zoom notes in an FAQ.

The AES 256-bit GCM encryption that’s being used is the same as Zoom currently uses but here combined with public key cryptography – which means the keys are generated locally, by the meeting host, before being distributed to participants, rather than Zoom’s cloud performing the key generating role.

“Zoom’s servers become oblivious relays and never see the encryption keys required to decrypt the meeting contents,” it explains of the E2EE implementation.

If you’re wondering how you can be sure you’ve joined an E2EE Zoom meeting a dark padlock will be displayed atop the green shield icon in the upper left corner of the meeting screen. (Zoom's standard GCM encryption shows a checkmark here.)

Meeting participants will also see the meeting leader's security code – which they can use to verify the connection is secure. "The host can read this code out loud, and all participants can check that their clients display the same code," Zoom notes.

33 Bringing a power tool from math into quantum computing

by Tokyo University of Science

https://phys.org/news/2020-10-power-tool-math-quantum.html

The Fourier transform is an important mathematical tool that decomposes a function or dataset into its constituent frequencies, much like one could decompose a musical chord into a combination of its notes. It is used across all fields of engineering in some form or another and, accordingly, algorithms to compute it efficiently have been developed – that is, at least for conventional computers. But what about quantum computers?

Though quantum computing remains an enormous technical and intellectual challenge, it has the potential to speed up many programs and algorithms immensely, provided that appropriate quantum circuits are designed. In particular, the Fourier transform already has a quantum version called the quantum Fourier transform (QFT), but its applicability is quite limited because its results cannot be used in subsequent quantum arithmetic operations.

To address this issue, in a recent study published in Quantum Information Processing, scientists from Tokyo University of Science developed a new quantum circuit that executes the quantum fast Fourier transform (QFFT) and fully benefits from the peculiarities of the quantum world. The idea for the study came to Mr. Ryo Asaka, first-year Master's student and one of the scientists on the study, when he first learned about the QFT and its limitations. He thought it would be useful to create a better alternative based on a variant of the standard Fourier transform called the fast Fourier transform (FFT), an indispensable algorithm in conventional computing that greatly speeds things up if the input data meets some basic conditions.

To design the quantum circuit for the QFFT, the scientists had to first devise quantum arithmetic circuits to perform the basic operations of the FFT, such as addition, subtraction, and digit shifting. A notable advantage of their algorithm is that no 'garbage bits' are generated; the calculation process does not waste any qubits, the basic unit of quantum information. Considering that increasing the number of qubits of quantum computers has been an uphill battle over the last few years, the fact that this novel quantum circuit for the QFFT can use qubits efficiently is very promising.

Another merit of their quantum circuit over the traditional QFT is that their implementation exploits a unique property of the quantum world to greatly increase computational speed. Associate Professor Kazumitsu Sakai, who led the study, explains: "In quantum computing, we can process a large amount of information at the same time by taking advantage of a phenomenon known as 'superposition of states.' This allows us to convert a lot of data, such as multiple images and sounds, into the frequency domain in one go." Processing speed is regularly cited as the main advantage of quantum computing, and this novel QFFT circuit represents a step in the right direction.

Moreover, the QFFT circuit is much more versatile than the QFT, as Assistant Professor Ryoko Yahagi, who also participated in the study, remarks: “One of the main advantages of the QFFT is that it is applicable to any problem that can be solved by the conventional FFT, such as the filtering of digital images in the medical field or analyzing sounds for engineering applications.” With quantum computers (hopefully) right around the corner, the outcomes of this study will make it easier to adopt quantum algorithms to solve the many engineering problems that rely on the FFT.

13 Oct 2020

34 The Importance of Cybersecurity and Protecting Quantum Technology Assets

by Kevin Coleman

https://thequantumdaily.com/2020/10/13/the-importance-of-cybersecurity-and-protecting-quantum-technology-assets/

In 2020 content published by the management consulting firm, McKinsey and Company, they stated that some companies may reap gains from quantum computing within five-years. There are some others that believe that this has already begun to happen. As quantum computing evolves and becomes more and more of a valuable business tool, it will undoubtably be brighter on the radar screen of cyber attackers and espionage agents. The theft and sale or use of the high-value information resulting from quantum computing problem solving will likely become a high value commodity on the black market and dark web. A cursory view of the current-state leads one to believe the industry needs to accelerate the evolution and use of cyber security protections (products and services) specifically addressing quantum technology platforms and operations.

The security threats to the digital data and communications of quantum computing is clearly growing in terms of likelihood and risk. Knowing what companies have begun leveraging the unique powers of quantum technology has value to their competitors and industry members. The ability to know the job (Problem) submitted for processing on a quantum computer has much more value from a competitive perspective. All of the major quantum computing platform providers offering access to the technology via the cloud must well versed and up-to-date in the area of protecting systems from cyberattacks. However, that is not the case for all the business users that are likely to be submitting work to quantum computing platforms! There is another cybersecurity issue relating to quantum computing. The ever-changing level of funding coupled with the current capabilities of quantum computers influence the likelihood that they will be able to crack the current encryption capabilities. No one knows when this will occur, it is impossible to predict at this point. It will happen sooner or later. Perhaps the best approach we can take is to prepare and remain up-to-date. Organizations should become proactive and adopt a defense forward mindset. The worst thing we can do is to ignore it until it is too late!

Think about the WEF article as it applies to protecting sensitive information about the development and use of quantum computing and technology in your field or industry. With the projected value of quantum computing and technology, they will undoubtably become high-value intellectual property targets for cyberattacks and espionage. After all, cyber security is the responsibility of everyone from the board of directors through each individual employee. This is why, in mid-July 2020, I asked a couple of the cybersecurity product and services vendors the following two questions.

“I have been working research involving protection of a quantum computing platform for a while now. I am interested in two things:

(i) Does your company have a product and or service to protect any of the quantum computing platforms? And if so what products and services for what platforms?

(ii) Do you have any near-term plans to create or expand cybersecurity coverage for quantum computing platforms and services?"

Some might see answering those questions a bit intrusive, since I have yet to receive any replies. You would think security companies would be very interested in defending the products and services in a new market niche that is currently projected to have a double-digit compound annual growth rate through 2025 resulting in billions in market value. A 2019 survey found that 30% of quantum computing business use cases has a 'high' estimated value! It was pointed out to me that there are multiple publicly traded quantum technology stocks currently on the open market. One has to wonder how they are meeting the cybersecurity expectations that accompany having investors and in a rigorously regulated investment environment.

The race to lead the quantum revolution is heated. Stealing competitors' quantum technology proprietary information is certainly one of the likely threats. The urgency of cybersecurity for quantum technology platforms, whether cloud based or in-house, must be addressed in order to mitigate the growing risks. It also supports the investment side of this rapidly growing market. The worst thing that could happen is the threats are ignored until a highly impactful breach takes place and makes the headlines globally.

35 The European Quantum Computing Startup Landscape

by Alex Kiltz

https://medium.com/uvc-partners-news/the-european-quantum-computing-startup-landscape-a115ffe84ad8

The upcoming years might very well be an exciting time to invest in quantum technologies. Below are some of the aspects that contribute to this belief.

Almost exactly a year ago, in October 2019, Google researchers claimed to have attained a pivotal quantum computing milestone (i.e., **quantum supremacy:** the point where quantum computers can do things that classical computers cannot) for the first time as noted in a paper published in Nature. Google's 53-qubit quantum computer, named Sycamore, took 200 seconds to perform a calculation that would have taken the world's fastest supercomputer 10,000 years.

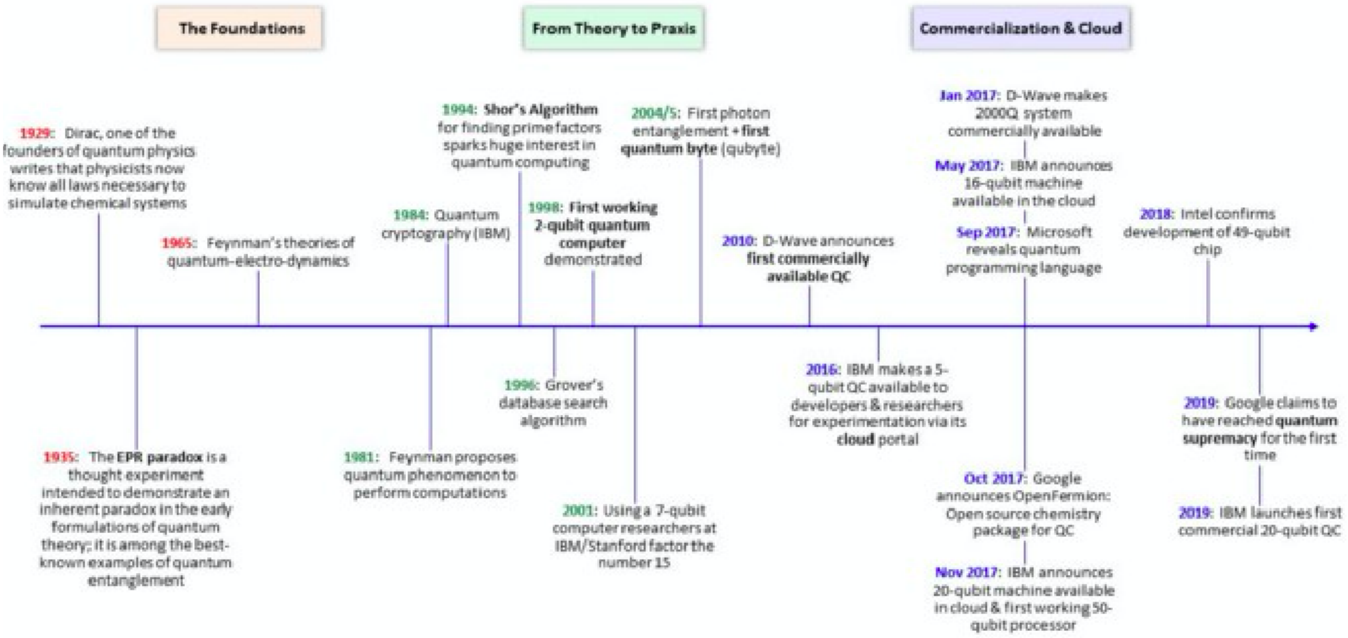
In more recent weeks, more exciting news came out of the quantum research labs of several companies: IBM announced its updated quantum roadmap and predicted to have developed a 1,000-qubit machine by 2023 (IBM's current quantum processor has 65 qubits). D-Wave revealed the launch of its new Advantage quantum computers based on a quantum annealing approach with over 5,000 qubits and made it available through its Leap cloud computing platform. Trapped-ion quantum computing startup IonQ claimed to have built the world's most powerful quantum computer yet with 32 qubits. European quantum computing startup IQM published a quantum computing breakthrough in Nature after having developed an ultra-sensitive nanoscale bolometer that detects very faint microwave radiation which can be used to measure the energy of photons (and thus the state of a superconducting qubit) much more accurately.

In this article, I won't dive into the fundamental quantum concepts such as decoherence, entanglement, superposition, or NISQ, but leave it to the experts to explain those concepts. Instead, I will focus on the quantum computing startup activity in Europe. However, before we examine the European quantum computing startup landscape, let's first develop a brief understanding of where the industry is at right now and the potential applications of quantum technology.

State of the Qubit – The Evolution of Quantum Technology

When describing the evolution of quantum technology, experts usually speak of a first and a second quantum revolution. In the first quantum revolution, which took place in the first half of the twentieth century, the field of quantum physics was created. In this period, the theoretical concepts and scientific foundations were established. The focus of this fundamental science has been on the discovery and control of quantum effects and properties. It led to the development of technologies such as lasers, transistors, solar cells, GPS, or medical imaging. Now, the second quantum revolution is underway. It builds on the premise of manipulating the individual states of single quantum particles such as photons, electrons, and atoms. Quantum mechanical concepts such as superposition, entanglement, and quantum correlations are harnessed. We are now at a point in time where the level of control of these phenomena is starting to be mature enough to be used for real-world quantum applications such as computing, secure communication, sensing, and simulation.

The figure below presents an overview of some of the milestones in the evolution of quantum technology with an emphasis on quantum computing.


The Foundations
From Theory to Praxis
Commercialization & Cloud
1929: Dirac, one of the founders of quantum physics writes that physicists now know all laws necessary to simulate chemical systems
1935: The EPR paradox is a thought experiment intended to demonstrate an inherent paradox in the early formulations of quantum theory; it is among the best-known examples of quantum entanglement
1965: Feynman's theories of quantum-electro-dynamics
1981: Feynman proposes quantum phenomenon to perform computations
1984: Quantum cryptography (IBM)
1994: Shor's Algorithm for finding prime factors sparks huge interest in quantum computing
1996: Grover's database search algorithm
1998: First working 2-qubit quantum computer demonstrated
2001: Using a 7-qubit computer researchers at IBM/Stanford factor the number 15
2004/5: First photon entanglement + first quantum byte (qubyte)
2010: D-Wave announces first commercially available QC
2016: IBM makes a 5-qubit QC available to developers & researchers for experimentation via its cloud portal
Jan 2017: D-Wave makes 2000Q system commercially available
May 2017: IBM announces 16-qubit machine available in the cloud
Sep 2017: Microsoft reveals quantum programming language
Oct 2017: Google announces OpenFermion: Open source chemistry package for QC
Nov 2017: IBM announces 20-qubit machine available in cloud & first working 50-qubit processor
2018: Intel confirms development of 49-qubit chip
2019: Google claims to have reached quantum supremacy for the first time
2019: IBM launches first commercial 20-qubit QC

Applications of Quantum Technology

There are three major applications of quantum technology: quantum communication, quantum sensing, and quantum computing.

(i) Quantum communication

Quantum communication encompasses the field of building ultra-secure communication systems. In recent years, a number of high-profile hacks have exposed sensitive information such as credit card details. Usually, sensitive data is encrypted and a digital key is required to decode the information. However, as these hacks show, the data can be corrupted when it is transmitted over fiber-optic cables. On top of that, hackers leave no traces when intercepting the information. Quantum communication, however, uses quantum physical properties to prevent this as hackers cannot intercept the data without being perceived. This approach leverages a concept called Quantum Key Distribution (QKD) which enables ultra-secure communication networks. Such networks allow the protected, digital transmission of sensitive data such as health records, financial transactions, or companies' proprietary information.

China is leading in the field of quantum communication. In 2017, it conducted the first-ever QKD-secured video conferencing call between Beijing and Vienna. This summer, China reached another milestone in quantum communications: Its Micius satellite (a Chinese satellite only dedicated to quantum communication) successfully established an ultra-secure communication link between two ground stations separated by more than 1000km.

(ii) Quantum sensing

Quantum sensing, or quantum metrology, uses quantum states for measurement and specifically their extreme sensitivity to disturbances. Because of that, quantum sensors can be used for highly sensitive measurement tasks where high precision is needed. This concept is already used in applications such as atomic clocks, laser distance meters, and magnetic resonance imaging for medical diagnosis. Now, individual quantum states can be manipulated to increase the sensitivity even further. This opens up an additional number of exciting use cases ranging from ultra-high precision microscopy, clocks, and positioning systems (e.g. for autonomous vehicles) to the detection of small doses of explosives, poisons, or raw materials deposits (e.g. rare earth elements) to below-cell-level medical imaging for less invasive diagnosis to brain-machine interfaces.

(iii) Quantum computing

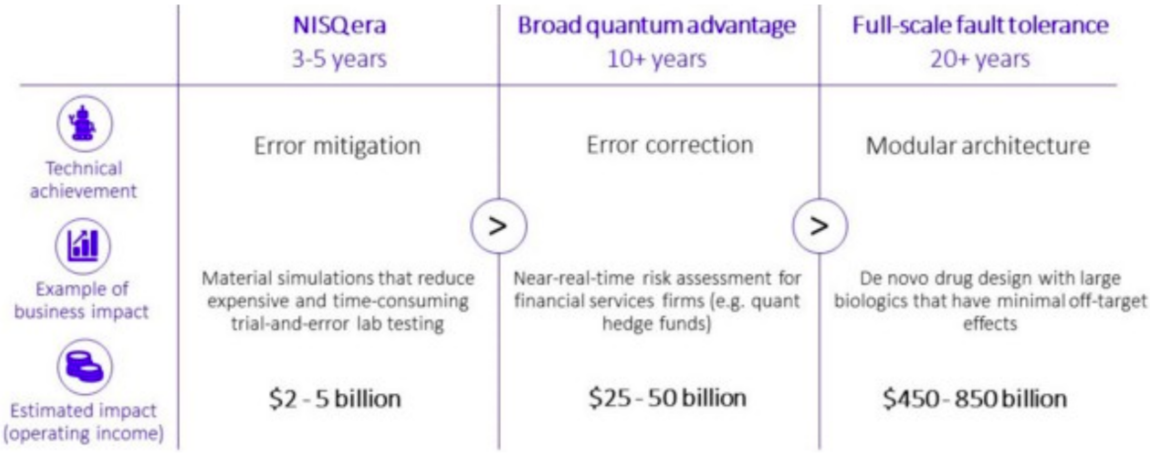
Quantum computers leverage the quantum mechanical properties of quantum bits, qubits, to achieve computing capabilities which promise to exceed those of today's most powerful supercomputers by magnitudes. Quantum computers are expected to accelerate computational tasks such as optimization problems, differential equations, linear algebra, and factorization. The following are some of the likely commercial applications:

- **pharma:** faster development of new drugs (how exciting in times of a pandemic!)
- **chemistry:** molecular simulation for the discovery of new materials (e.g. for battery cells and fertilizers)
- **fluid dynamics** simulation for automotive and aerospace applications
- **network optimization** (e.g. for most efficient traffic routing to combat congestion and emissions)
- **cryptography and cybersecurity**
- **weather forecasting** and climate change
- **chip layout optimization** in the semiconductor industry
- **finance:** risk management, portfolio optimization, and market simulation
- **supply chain optimization** (e.g. most efficient planning and routing)
- **marketing and customer segmentation**

To illustrate the advantages of quantum computers compared to conventional computers, let's take penicillin as an example of a drug discovery process in pharma:

> "For scientists trying to design a compound that will attach itself to, and modify, a target disease pathway, the critical first step is to determine the electronic structure of the molecule. But modeling the structure of a molecule of an everyday drug such as penicillin, which has 41 atoms at ground state, requires a classical computer with some 1086 bits – more transistors than there are atoms in the observable universe. Such a machine is a physical impossibility. But for quantum computers, this type of simulation is well within the realm of possibility, requiring a processor with 286 quantum bits, or qubits."

Quantum computing is maturing with the advent of more powerful quantum processors with an increasing number of qubits, longer coherence times and gate fidelities, more developer tools such as compilers and libraries, and better algorithms suited for quantum computing (e.g. Shor's or Grover's). The addressability of the aforementioned applications will largely depend on the sophistication of the underlying technology. Hence, with a maturing quantum technology being able to address more and more complex applications, the corresponding commercial impact will increase x-fold. While the specific timing is still unknown, as the following figure shows, the resulting business value is expected to be tremendous and could well be in the hundreds of billions of dollars.



	NISQ era 3-5 years	Broad quantum advantage 10+ years	Full-scale fault tolerance 20+ years
Technical achievement	Error mitigation	Error correction	Modular architecture
Example of business impact	Material simulations that reduce expensive and time-consuming trial-and-error lab testing	Near-real-time risk assessment for financial services firms (e.g. quant hedge funds)	De novo drug design with large biologics that have minimal off-target effects
Estimated impact (operating income)	$2 - 5 billion	$25 - 50 billion	$450 - 850 billion

The European Quantum Computing Startup Landscape

By diving into the European quantum computing startup landscape, I will mostly focus on the application of quantum computing and aim at answering the following questions: What are the recent developments in quantum science? What are the leading research institutes for quantum technologies across Europe? What does the current startup activity in quantum technologies look like? Which are the different funding mechanisms that are available for startups in the field? How do funding levels differ across categories and countries? What are the most attractive market segments from a VC point of view? Below is a summary of some of the findings.

- **Methodology**

  To analyze the European quantum computing startup ecosystem, data sources such as Crunchbase, Tracxn, company announcements, and press releases as well as UVC Partners' deal flow were used.

For funding levels, only publicly available equity funding data (i.e. no public grants) was considered. The startups were selected according to the following criteria: founded after 2010 and headquartered in Europe (including Israel, Russia, and Turkey). Companies that went out of business and where the primary application was not quantum computing-related (e.g. research and consulting firms) were eliminated from the sample. Over 270 startups were initially identified and 69 qualified according to the described criteria.

- **A Bird's View**

  The 69 European quantum computing startups that were founded since 2010 raised a total of just over €150m to date. Only one exit was recorded, albeit from a company founded in 2001: ID Quantique was acquired by SK Telecom for €55m in 2018.

  When looking at the geographical spread of startups across Europe, the UK leads the scoreboard with 23 startups followed by Germany (13), France (7), Spain and Switzerland (4 each), and Finland and The Netherlands (3 each). As expected, three cities from the UK are among the top five cities in terms of the number of startups: London (8), Cambridge (3), and Oxford (2). Three startups in our sample are from Berlin. Barcelona, Helsinki, Innsbruck, Lausanne, and Munich are home to two startups each.

  Unsurprisingly, UK startups raised the most funding (€85m), followed by Finland (€27m), Israel (€20m), and Switzerland (€12m). Quantum computing startups in France (€3m) raised significantly less. However, it has to be noted that these numbers are driven by a few outliers which are the most funded startups in Europe to date in terms of publicly disclosed equity funding: Cambridge Quantum Computing (€44.3m; Cambridge, UK), IQM (€26.5m; Espoo, Finland), Quantum Machines (€19.5m; Tel Aviv, Israel), Terra Quantum (€10.0m; Rorschach, Switzerland), and Quantum Motion Technologies (€8.7m; Leeds, UK).

- **Category Deep Dives**

  Hardware startups are segmented in two subcategories (yes, some startups could fall in various clusters): Computing and Components & Materials. The 25 hardware startups raised a total of €47.6m to date.

  Hardware – Computing

  - Definition: startups that are developing hardware products specifically dedicated to the computing function of quantum computers
  - Number of startups: 12
  - Total funding: €42.1m
  - Most funded company: IQM (Espoo, Finland), €26.5m
  - Examples: IQM, and Quantum Motion Technologies

  IQM develops superconducting quantum computers with application-specific processors in a hardware-software co-design approach. The hardware is based on a proprietary chip technology that allows them to significantly speed up the clock speed of quantum processors. The ultimate goal is to deploy their quantum computers on-premise at their customers' facilities. IQM is a spin-out from Aalto University and VTT.

  UK-based **Quantum Motion Technologies** develops silicon spin-based qubit architectures for fault-tolerant quantum processors that are compatible with standard CMOS fabrication and, therefore, potentially easier to scale to thousands or even millions of qubits. The silicon spin technology and architectures were developed at University College London and at Oxford University.

Hardware – Components & Materials

- Definition: startups that are working on peripheral technologies of quantum computers such as cryogenics
- Number of startups: 13
- Total funding: €5.5m
- Most funded company: Nu Quantum (Cambridge, UK), €3.1m
- Examples: kiutra, and Nu Quantum

Germany-based **kiutra** is a spin-off from the Technical University of Munich and commercializes cryogen-free (and, thus, helium-3 free) refrigeration systems based on a magnetic cooling approach. In contrast to other commercial magnetic refrigerators, their modular technical approach allows for continuous cooling at sub-Kelvin temperatures.

Nu Quantum, a quantum photonics spin-off from the University of Cambridge, develops single-photon components to enable the next generation of commercially-viable photonic quantum technologies. The startup uses nano-engineered materials to make quantum devices that can emit and detect single-photons. The devices can operate at room temperature and have the future capability of fitting multiple on a chip. As a first use case, Nu Quantum will deploy the technology to generate random numbers to be used for cryptographic keys to secure data.

Software startups are segmented in the two subcategories Operating Systems and Applications. The 44 software startups raised a total of €103.0m.

Software – Operating Systems

- Definition: startups that are developing quantum operating systems, compilers, and quantum programming languages and tools
- Number of startups: 5
- Total funding: €23.4m
- Most funded company: Quantum Machines (Tel Aviv, Israel), €19.5m
- Examples: Quantum Machines, and Riverlane

Israel-based Quantum Machines brings a quantum orchestration platform to the market. It is a combination of custom hardware and software tools that can be used to control virtually any available quantum processor (superconducting, trapped-ion, etc.). The startup built a proprietary pulse processor that can handle multi-qubit manipulation. On top of that, Quantum Machines developed software to write algorithms in the startup's QUA programming language.

Riverlane, a spin-out from the University of Cambridge, develops software that transforms quantum computers from experimental technology into commercial products. The startup commercializes a new operating system for quantum computers. Inspired by heterogeneous architectures, its operating system makes all computing elements in the stack accessible – CPU, FPGAs, and qubits. This empowers quantum programmers to implement fast operations at the right level in the stack. Its operating system comes with its own programming language and application library.

Software – Applications

Application software startups are further grouped in three subgroups: Security & Encryption (19 startups, €19.6m total funding), Chemistry & Pharma (11 startups, €48.7m total funding), and Other application software startups (9 startups, €11.3m total funding).

- Definition: startups that are working on quantum computing application software targeted at various use cases and industries
- Number of startups: 39
- Total funding: €79.6m
- Most funded company: Cambridge Quantum Computing (Cambridge, UK), €44.3m
- Examples: HQS Quantum Simulations, and Rahko

Germany-based **HQS Quantum Simulations**, a spin-off from the Karlsruhe Institute of Technology, predicts the properties of molecules and materials using quantum computers and thereby accelerates development cycles in the chemistry and pharma industries. While current quantum computers suffer from intrinsic errors that limit their performance, HQS develops algorithms that can deal with these errors and enable customers to profit from the performance advantage of quantum computers earlier than their competitors. In addition, the company offers individual simulation solutions for conventional computers with the integration of high-end simulation methods and the possibility to utilize them with upcoming quantum computers.

Rahko, a UK-based startup associated with University College London, applies machine learning to quantum computing for chemical simulations. The company specializes in quantum machine learning for faster and more accurate simulation of drugs and materials for the discovery and development of new molecules and materials at a greatly reduced cost. The current models developed by Rhako will also be able to be deployed in future quantum computers, once the devices are at scale.

European Quantum Computing Research Hotspots & Initiatives

Europe has a long-standing tradition and expertise in quantum research which dates back to the origins of quantum physics in the first decades of the 20th century. Its excellent research universities are a well-respected breeding ground of international quantum talent. Europe's focus on a range of different fields in quantum technologies enables collaboration across research institutes as well as across borders, which in turn fosters interdisciplinary innovation.

Thus, and given the research-heavy nature of quantum computing, there is a strong link between the startup activity in this field and research institutes. Most startups are direct spin-offs from research groups such as AQT (University of Innsbruck), Delft Circuits (TU Delft), HQS Quantum Simulations (Karlsruhe Institute of Technology), IQM (Aalto University & VTT), Oxford Quantum Circuits (University of Oxford), or Qilimanjaro Quantum Tech (University of Barcelona).

Public Funding for Quantum Technologies in Europe

While Europe has a long history of financing research in quantum technologies, funding from industry players was highly selective over the past decades and limited to companies in the areas of computing, laser, and telecommunication. However, driven by technological advances in recent years, the industry has rediscovered its interest in quantum technologies. Companies are increasingly looking to integrate those technologies into their products or to use it for internal R&D efforts.

As presented above, private funding (i.e. venture capital) into startups commercializing quantum technologies is rather limited in Europe compared to the capital investment in North America. Fortunately, the situation looks different when examining public funding levels: Through the Quantum Flagship initiative under the Horizon 2020 research framework program, the European Union committed €1 billion for quantum research projects over the period 2018-2028. Moreover, Germany recently announced €2 billion for the development and set-up of at least two quantum computers in the country. In comparison, from 2019 to 2028, the United States will invest $1.2 billion into quantum technologies. However, this is dwarfed by China which will spend about $10 billion for its new National Laboratory for Quantum Information Sciences.

Quantum technologies have become of high geopolitical relevance which is why there is an ongoing global race to conquer the market and to secure key know-how and technologies. For European startups to thrive in an environment of limited private funding, surely more public funding will be required to help commercialize quantum technologies being developed by leading European research institutions.

The Next Quantum Leap

The next few years could be a pivotal point in time when quantum science is advanced enough to make its way from research labs into real-world applications in fields such as quantum communication and sensing as well as quantum computers itself. Given the massive impact these quantum technologies could have, I'm extremely excited about recent developments and what the quantum future will bring. Just like it was unimaginable 20 years ago the kinds of innovation an iPhone could bring with it, I'm positive quantum technologies will bring with them an even larger plethora of new use cases and applications. Thus, I believe there are plenty of exciting opportunities for startups.

12 Oct 2020

36 How to build up cybersecurity for medical devices

by Zeljka Zorz

https://www.helpnetsecurity.com/2020/10/12/how-to-build-up-cybersecurity-for-medical-devices/

Manufacturing medical devices with cybersecurity firmly in mind is an endeavour that, according to Christopher Gates, an increasing number of manufacturers is trying to get right.

Healthcare delivery organizations have started demanding better security from medical device manufacturers (MDMs), he says, and many have have implemented secure procurement processes and contract language for MDMs that address the cybersecurity of the device itself, secure installation, cybersecurity support for the life of the product in the field, liability for breaches caused by a device not following current best practice, ongoing support for events in the field, and so on.

"For someone like myself who has been focused on cybersecurity at MDMs for over 12 years, this is excellent progress as it will force MDMs to take security seriously or be pushed out of the market by competitors who do take it seriously. Positive pressure from MDMs is driving cybersecurity forward more than any other activity," he told Help Net Security.

Gates is a principal security architect at Velentium and one of the authors of the recently released Medical Device Cybersecurity for Engineers and Manufacturers, a comprehensive guide to medical device secure lifecycle management, aimed at engineers, managers, and regulatory specialists.

In this interview, he shares his knowledge regarding the cybersecurity mistakes most often made by manufacturers, on who is targeting medical devices (and why), his view on medical device cybersecurity standards and initiatives, and more.

Are attackers targeting medical devices with a purpose other than to use them as a way into a healthcare organization's network?

The easy answer to this is "yes," since many MDMs in the medical device industry perform "competitive analysis" on their competitors' products. It is much easier and cheaper for them to have a security researcher spend a few hours extracting an algorithm from a device for analysis than to spend months or even years of R&D work to pioneer a new algorithm from scratch.

Also, there is a large, hundreds-of-millions-of-dollars industry of companies who "re-enable" consumed medical disposables. This usually requires some fairly sophisticated reverse-engineering to return the device to its factory default condition.

Lastly, the medical device industry, when grouped together with the healthcare delivery organizations, constitutes part of critical national infrastructure. Other industries in that class (such as nuclear power plants) have experienced very directed and sophisticated attacks targeting safety backups in their facilities. These attacks seem to be initial testing of a cyber weapon that may be used later.

While these are clearly nation-state level attacks, you have to wonder if these same actors have been exploring medical devices as a way to inhibit our medical response in an emergency. I'm speculating: we have no evidence that this has happened. But then again, if it has happened there likely wouldn't be any evidence, as we haven't been designing medical devices and infrastructure with the ability to detect potential cybersecurity events until very recently.

What are the most often exploited vulnerabilities in medical devices?

It won't come as a surprise to anyone in security when I say "the easiest vulnerabilities to exploit." An attacker is going to start with the obvious ones, and then increasingly get more sophisticated. Mistakes made by developers include:

Unsecured firmware updating

I personally always start with software updates in the field, as they are so frequently implemented incorrectly. An attacker's goal here is to gain access to the firmware with the intent of reverse-engineering it back into easily-readable source code that will yield more widely exploitable vulnerabilities (e.g., one impacting every device in the world). All firmware update methods have at least three very common potential design vulnerabilities. They are:

- Exposure of the binary executable (i.e., it isn't encrypted)
- Corrupting the binary executable with added code (i.e., there isn't an integrity check)
- A rollback attack which downgrades the version of firmware to a version with known exploitable vulnerabilities (there isn't metadata conveying the version information).

Overlooking physical attacks

Physical attack can be mounted:

- Through an unsecured JTAG/SWD debugging port
- Via side-channel (power monitoring, timing, etc.) exploits to expose the values of cryptographic keys
- By sniffing internal busses, such as SPI and I2C
- Exploiting flash memory external to the microcontroller (a $20 cable can get it to dump all of its contents)

Manufacturing support left enabled

Almost every medical device needs certain functions to be available during manufacturing. These are usually for testing and calibration, and none of them should be functional once the device is fully deployed. Manufacturing commands are frequently documented in PDF files used for maintenance, and often only have minor changes across product/model lines inside the same manufacturer, so a little experimentation goes a long way in letting an attacker get access to all kinds of unintended functionality.

No communication authentication

Just because a communications medium connects two devices doesn't mean that the device being connected to is the device that the manufacturer or end-user expects it to be. No communications medium is inherently secure; it's what you do at the application level that makes it secure.

Bluetooth Low Energy (BLE) is an excellent example of this. Immediately following a pairing (or re-pairing), a device should always, always perform a challenge-response process (which utilizes cryptographic primitives) to confirm it has paired with the correct device.

I remember attending an on-stage presentation of a new class II medical device with a BLE interface. From the audience, I immediately started to explore the device with my smartphone. This device had no authentication (or authorization), so I was able to perform all operations exposed on the BLE connection. I was engrossed in this interface when I suddenly realized there was some commotion on stage as they couldn't get their demonstration to work: I had accidentally taken over the only connection the device supported. (I then quickly terminated the connection to let them continue with the presentation.)

What things must medical device manufacturers keep in mind if they want to produce secure products?

There are many aspects to incorporating security into your development culture. These can be broadly lumped into activities that promote security in your products, versus activities that convey a false sense of security and are actually a waste of time.

Probably the most important thing that a majority of MDMs need to understand and accept is that their developers have probably never been trained in cybersecurity. Most developers have limited knowledge of how to incorporate cybersecurity into the development lifecycle, where to invest time and effort into securing a device, what artifacts are needed for premarket submission, and how to proper utilize cryptography. Without knowing the details, many managers assume that security is being adequately included somewhere in their company's development lifecycle; most are wrong.

To produce secure products, MDMs must follow a secure "total product life cycle," which starts on the first day of development and ends years after the product's end of life or end of support.

They need to:

- Know the three areas where vulnerabilities are frequently introduced during development (design, implementation, and through third-party software components), and how to identify, prevent, or mitigate them
- Know how to securely transfer a device to production and securely manage it once in production
- Recognize an MDM's place in the device's supply chain: not at the end, but in the middle. An MDMs cybersecurity responsibilities extend up and down the chain. They have to contractually enforce cybersecurity controls on their suppliers, and they have to provide postmarket support for their devices in the field, up through and after end-of-life
- Create and maintain Software Bills of Materials (SBOMs) for all products, including legacy products. Doing this work now will help them stay ahead of regulation and save them money in the long run.

They must avoid mistakes like:

- Not thinking that a medical device needs to be secured
- Assuming their development team 'can' and 'is' securing their product
- Not designing-in the ability to update the device in the field
- Assuming that all vulnerabilities can be mitigated by a field update
- Only considering the security of one aspect of your design (e.g., its wireless communication protocol). Security is a chain: for the device to be secure, all the links of the chain need to be secure. Attackers are not going to consider certain parts of the target device 'out of bounds' for exploiting.

Ultimately, security is about protecting the business model of an MDM. This includes the device's safety and efficacy for the patient, which is what the regulations address, but it also includes public opinion, loss of business, counterfeit accessories, theft of intellectual property, and so forth. One mistake I see companies frequently make is doing the minimum on security to gain regulatory approval, but neglecting to protect their other business interests along the way - and those can be very expensive to overlook.

What about the developers? Any advice on skills they should acquire or brush up on?

First, I'd like to take some pressure off developers by saying that it's unreasonable to expect that they have some intrinsic knowledge of how to implement cybersecurity in a product. Until very recently, cybersecurity was not part of traditional engineering or software development curriculum. Most developers need additional training in cybersecurity.

And it's not only the developers. More than likely, project management has done them a huge disservice by creating a system-level security requirement that says something like, "Prevent ransomware attacks." What is the development team supposed to do with that requirement? How is it actionable?

At the same time, involving the company's network or IT cybersecurity team is not going to be an automatic fix either. IT Cybersecurity diverges from Embedded Cybersecurity in many respects, from detection to implementation of mitigations. No MDM is going to be putting a firewall on a device that is powered by a CR2032 battery anytime soon; yet there are ways to secure such a low-resource device.

In addition to the how-to book we wrote, Velentium will soon offer training available specifically for the embedded device domain, geared toward creating a culture of cybersecurity in development teams. My audacious goal is that within 5 years every medical device developer I talk to will be able to converse intelligently on all aspects of securing a medical device.

What cybersecurity legislation/regulation must companies manufacturing medical devices abide by?

It depends on the markets you intend to sell into. While the US has had the Food and Drug Administration (FDA) refining its medical device cybersecurity position since 2005, others are more recent entrants into this type of regulation, including Japan, China, Germany, Singapore, South Korea, Australia, Canada, France, Saudi Arabia, and the greater EU.

While all of these regulations have the same goal of securing medical devices, how they get there is anything but harmonized among them. Even the level of abstraction varies, with some focused on processes while others on technical activities.

But there are some common concepts represented in all these regulations, such as:

- Risk management
- Software bill of materials (SBOM)
- Monitoring
- Communication
- "Total Product Lifecycle"
- Testing

But if you plan on marketing in the US, the two most important document should be FDA's:

- 2018 – Draft Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- 2016 – Final Guidance: Postmarket Management of Cybersecurity in Medical Devices (The 2014 version of the guidance on premarket submissions can be largely ignored, as it no longer represents the FDA's current expectations for cybersecurity in new medical devices).

What are some good standards for manufacturers to follow if they want to get cybersecurity right?

The Association for the Advancement of Medical Instrumentation's standards are excellent. I recommend AAMI TIR57: 2016 and AAMI TIR97: 2019.

Also very good is the Healthcare & Public Health Sector Coordinating Council's (HPH SCC) Joint Security Plan. And, to a lesser extent, the NIST Cyber Security Framework.

The work being done at the US Department of Commerce / NTIA on SBOM definition for vulnerability management and postmarket surveillance is very good as well, and worth following.

What initiatives exist to promote medical device cybersecurity?

Notable initiatives I'm familiar with include, first, the aforementioned NTIA work on SBOMs, now in its second year. There are also several excellent working groups at HSCC, including the Legacy Medical Device group and the Security Contract Language for Healthcare Delivery Organizations group. I'd also point to numerous working groups in the H-ISAC Information Sharing and Analysis Organization (ISAO), including the Securing the Medical Device Lifecycle group.

And I have to include the FDA itself here, which is in the process of revising its 2018 premarket draft guidance; we hope to see the results of that effort in early 2021.

What changes do you expect to see in the medical devices cybersecurity field in the next 3-5 years?

So much is happening at high and low levels. For instance, I hope to see the FDA get more of a direct mandate from Congress to enforce security in medical devices.

Also, many working groups of highly talented people are working on ways to improve the security posture of devices, such as the NTIA SBOM effort to improve the transparency of software "ingredients" in a medical device, allowing end-users to quickly assess their risk level when new vulnerabilities are discovered.

Semiconductor manufacturers continue to give us great mitigation tools in hardware, such as side-channel protections, cryptographic accelerators, virtualized security cores. Trustzone is a great example.

And at the application level, we'll continue to see more and better packaged tools, such as cryptographic libraries and processes, to help developers avoid cryptography mistakes. Also, we'll see more and better process tools to automate the application of security controls to a design.

HDOs and other medical device purchasers are better informed than ever before about embedded cybersecurity features and best practices. That trend will continue, and will further accelerate demand for better-secured products.

I hope to see some effort at harmonization between all the federal, state, and foreign regulations that have been recently released with those currently under consideration.

One thing is certain: legacy medical devices that can't be secured will only go away when we can replace them with new medical devices that are secure by design. Bringing new devices to market takes a long time. There's lots of great innovation underway, but really, we're just getting started!

11 Oct 2020

37 Five Eyes governments, India, and Japan make new call for encryption backdoors

by Catalin Cimpanu

https://www.zdnet.com/article/five-eyes-governments-india-and-japan-make-new-call-for-encryption-backdoors/

Members of the intelligence-sharing alliance Five Eyes, along with government representatives for Japan and India, have published a statement over the weekend calling on tech companies to come up with a solution for law enforcement to access end-to-end encrypted communications.

The statement is the alliance's latest effort to get tech companies to agree to encryption backdoors.

The Five Eyes alliance, comprised of the US, the UK, Canada, Australia, and New Zealand, have made similar calls to tech giants in 2018 and 2019, respectively.

Just like before, government officials claim tech companies have put themselves in a corner by incorporating end-to-end encryption (E2EE) into their products.

If properly implemented, E2EE lets users have secure conversations – may them be chat, audio, or video – without sharing the encryption key with the tech companies.

Representatives from the seven governments argue that the way E2EE encryption is currently supported on today's major tech platforms prohibits law enforcement from investigating crime rings, but also the tech platforms themselves from enforcing their own terms of service.

Signatories argue that "particular implementations of encryption technology" are currently posing challenges to law enforcement investigations, as the tech platforms themselves can't access some communications and provide needed data to investigators.

This, in turn, allows a safe haven for criminal activity and puts the safety of "highly vulnerable members of our societies like sexually exploited children" in danger, officials argued.

"We call on technology companies to work with governments to take the following steps, focused on reasonable, technically feasible solutions," the seven governments said in a press release.

- "Embed the safety of the public in system designs, thereby enabling companies to act against illegal content and activity effectively with no reduction to safety, and facilitating the investigation and prosecution of offences and safeguarding the vulnerable;
- Enable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight; and
- Engage in consultation with governments and other stakeholders to facilitate legal access in a way that is substantive and genuinely influences design decisions."

Officials said they are committed to working with tech companies on developing a solution that allows users to continue using secure, encrypted communications, but also allows law enforcement and tech companies to crack down on criminal activity.

The seven governments called for encryption backdoors not only in encrypted instant messaging applications, but also for "device encryption, custom encrypted applications, and encryption across integrated platforms."

In December 2018, Australia was the first major democratic country to introduce an encryption-busting law.

Similar efforts have also taken place in the US and Europe, but were less successful, primarily due to opposition from either tech companies, non-profits, or the general public.

However, pressure has been mounting in recent years as western governments seek to reach intelligence-gathering parity with China.

09 Oct 2020

38 HOW TO ANTICIPATE THE PROTECTION OF YOUR DATA IN THE POST-QUANTUM ERA?

https://blog.ercom.com/how-to-anticipate-the-protection-of-your-data-in-the-post-quantum-era/

In the 1990s, scientific researchers predicted that if a very powerful computer came on the market, it would be able to decipher encrypted business or government data in record time. If you never heard of the quantum computer project, you should know that for some people, it would be considered the greatest threat to data security, while for others, the quantum computer is just a myth, dreamed up by hackers, which may never see the light of day. Explanations of post-quantum cryptography . . .

What is a quantum computer?

Thanks to these two phenomena, **superposition** and **entanglement**, a quantum computer can theoretically access all the possible results of a calculation in a single step, whereas a conventional computer has to process information sequentially, one result after the other. This massive parallelism is at the heart of the power of the quantum computer.

What about cryptography? Cryptography uses several “principles, means and methods of data transformation, with the aim of hiding their content, preventing their modification from going unnoticed and/or preventing their unauthorized use.”

In particular, public-key cryptography allows two parties to authenticate each other or exchange a secret key over a network. This secret key is then used in a number of common secure services and platforms (online payment, instant messaging, communication, document storage, videoconferencing, transportation card . . .) and millions of businesses use it. Public key cryptography is designed to protect all your personal and business data, and is now an integral part of the digital economy.

To date, cyber-security experts are able to counter all kinds of cryptographic attacks by increasing the size of security keys. But eventually this method will become obsolete. While conventional computers can “theoretically” take billions of years to decipher encrypted data using well-established algorithms, the acceleration in computing power enabled by the quantum computer could cause conventional encryption methods to fall apart.

As introduced above, a quantum computer can decipher any encrypted data using standard cryptography. This is why, in response to the possible emergence of a quantum computer on the market, standard cryptography is adapting and becoming “post-quantum cryptography”. It is based on “new mathematical concepts to encrypt communication protocols" and "can resist the power of a quantum computer".

The quantum computer, an invisible but powerful threat

Digital giants such as IBM, Google and Intel are competing to lead on the quantum field, and are actively working on powerful computers that can offer ever higher computing capabilities. IBM has just published its quantum roadmap and claims it will have a 1000-bit machine by 2023. The stakes are high: Anne Canteaut, a computer scientist specialized in cryptography, believes there is a 50% chance that one of the cryptographic systems based on a shared public key, used in all transactions around the world, will be broken within the next fifteen years using a quantum computer.

The threat is deemed so serious that NIST, the main American standardization body, has decided to scrap standards based on public-key cryptography in favor of new quantum-resistant standards. According to the NIST roadmap, these new standards should arrive by 2022. This trend is international. In France, for example, ANSSI already recommends taking these new standards into account to protect data with a long lifespan.

For their part, organizations must now anticipate possible future attacks by strengthening the protection of their encrypted data in order to secure it over the long or even very long term. Some confidential information require protection over several decades, up to 60 years for the most sensitive (government applications, air fleets, social security cards and healthcare data, electronic signatures, confidential communications . . .), even up to 100 years for a notarial deed regarding a minor!

Successful attacks by a quantum computer would involve compromising the identity of certain information sources, disclosing intellectual and industrial property titles, non-repudiation of legal documents by forging signatures, or the unencrypted dissemination of our confidential data history.

Regardless of their industry, organizations must develop solutions to counter possible cyber-attacks orchestrated using a quantum computer, and allocate the necessary investments in robust infrastructures, dedicated hardware and secure tools (specific hardware, key exchanges, etc.).

How to respond to potential quantum computer attacks?

Unveiled at the beginning of September 2020 by the French government, the recovery plan will allocate €7 billion to the digital industry, out of the €100 billion announced. An industry considered strategic and essential for the future of the country. Details:

- €2.4 billion will be devoted to French technological sovereignty (via investments in areas such as quantum computing, cyber-security, artificial intelligence, the Cloud, digital healthcare, etc).
- €2.3 billion will go towards accelerating the digital transition of businesses and government services (securing infrastructures, digitization of the healthcare system, etc.).
- €1.3 billion will be earmarked for the development of start-ups (through aid for innovation under the Future Investment Program and participation in fund-raisers).

These investments are necessary to accelerate the deployment of new post-quantum cryptography standards to all the solutions and secure platforms of our daily professional and personal lives.

Post-quantum cryptography already exists on the market, even before the appearance of the quantum computer. Digital players are developing new algorithms, integrated into professional solutions, resistant to all kinds of external attacks against secure communications, storage and exchange of sensitive information.

In France, CryptoNext Security offers new cryptography standards to secure information systems against attacks. In a partnership with Ercom, the two French companies were able to develop a first post-quantum integration test using the library developed by CryptoNext Security (Quantum-Safe library) in Ercom's Cryptosmart solution to secure mobile devices and communications. Integration was quickly done due to the simplicity offered by the Cryptonext Security library and Cryptosmart's architecture designed to evolve easily. As a result, the first users were able to make post-quantum calls safely! A technological and secure breakthrough addressing the strategic and sovereign challenges of organizations in all industries.

This "historic update"now needs to be applied to all our devices to ensure total protection of our digital economy against the threat of the quantum computer.

39 Visa, JPMorgan Are Already Preparing for Potential Quantum Cyberattacks

by Sara Castellanos

https://www.wsj.com/articles/visa-jpmorgan-are-already-preparing-for-potential-quantum-cyberattacks-11602255213

Financial services companies are preparing for a time when a powerful quantum computer could break some of the most widespread cryptographic methods currently used in cybersecurity.

Experts say quantum-computing cyberattacks could be more than a decade away, based on the technology's rate of progress, but the consequences could be so severe that companies and cryptographers world-wide are preparing now. Visa Inc. and JPMorgan Chase & Co., for example, are researching methods capable of thwarting such an attack, developing new processes and closely following the race for new encryption standards.

"The data we have is sensitive, and it is vast in quantity, so protecting that data is job number one for us," said Rajat Taneja, president of technology at Visa.

Nearly six years ago, researchers at Visa began studying so-called post-quantum cryptography, which refers to the new cryptographic methods that could be used to withstand an attack from a quantum computer.

Researchers at Visa have published four peer-reviewed papers about cryptographic systems that could be used against a quantum-computing attack, and a fifth is in the works, Mr. Taneja said. Dozens of security experts and software engineers across the firm have contributed to the research.

Quantum computers are still in the early stages of development. The machines harness the properties of quantum physics, including superposition and entanglement, to radically speed up complex calculations related to finance, health care and manufacturing that are intractable for today's computers. While traditional computers store information as either zeros or ones, quantum computers use quantum bits, or qubits, which represent and store information as both zeros and ones simultaneously.

Some researchers estimate that it would take a machine with 250 million qubits to break today's public-key cryptography, a widely used encryption method that could be particularly vulnerable.

While today's early-stage quantum computers are far less powerful, much of the financial industry is secured by public-key cryptography, ranging from online banking and online transactions to banking mobile apps, Mr. Taneja said.

A popular public-key cryptography method, RSA, would be especially at risk. RSA is vulnerable to quantum computers because it is based on integer factorization, which is essentially reverse multiplication, using numbers that can be about 1,000 digits long.

Regular computers – even supercomputers – can't factor such long numbers fast enough to beat these defenses. Quantum computers, though, may be able to solve integer factorization problems many millions of times faster.

Security experts and the companies developing quantum computers, such as Alphabet Inc.'s Google and Microsoft Corp. , have been aware of the threat for years. Hundreds of the world's top cryptographers are involved in a competition to develop new encryption standards for the U.S., which would guard against both classical and quantum-computing cyberattacks.

A quantum computing attack could compromise not only data in the path of the attack but also the digital-signature algorithms used to verify the identity of some secure websites, said Yassir Nawaz, an executive director at JPMorgan responsible for securing emerging technologies at the bank.

That could allow bad actors to create fake identities for websites, as well as fake software downloads and software updates. JPMorgan executives have been aware of the threat for years, he said. "We've been actively discussing within the firm as to how we'd address this," Mr. Nawaz said. "But the reality is that this is something that affects the entire ecosystem."

JPMorgan is developing processes to help identify high-priority data sets that need to be protected for several years and could be at risk if a powerful quantum computer becomes available, Mr. Nawaz said. "We need to have a process that lets us identify and inventory that data," he said.

That data would then be first in line to be secured by new encryption standards that could withstand a quantum cyberattack, he said. New encryption standards are being developed now, in a cryptography competition led by the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce.

Visa and JPMorgan plan to begin adopting NIST's new standards when they become available, which will require coordination with industry organizations. It can take as long as 15 years for internet activity to be secured by the new encryption methods, experts say.

"I don't believe one day we'll flip a switch and everything will be post-quantum (encryption)," Mr. Nawaz said. "It's going to take a long time, starting with the high-risk data."

40 How the enterprise can shut down cyber criminals and protect a remote staff

by N.F. Mendoza

https://www.techrepublic.com/article/how-the-enterprise-can-shut-down-cyber-criminals-and-protect-a-remote-staff/

Hackers accidentally allowed into company software by security noncompliant employees cost businesses millions annually; we asked experts to weigh in on best safety practices.

Cyber threats didn't suddenly become a thing when COVID-19 pushed the enterprise into a remote workforce. Careless, security noncompliant employees have negligently allowed hackers access into company computers and software while solidly ensconced within a brick-and-mortar office. A pre-US lockdown January insider threats report from Ponemon showed the average global cost of those insider threats rose 31% from 2018 to when the report was compiled on Jan 29, and incidents of hacking spiked 47% in the same time period.

Hacking has gone viral

But the coronavirus pandemic brought a new slew of cyber threats, feeding on how "Anxiety and desperation can make it easy to let one's guard down when it comes to online threats," Forcepoint principal security analyst Carl Leonard told TechRepublic in March.

Last month, TechRepublic's sister-site ZDNet reported what it dubbed "disturbing statistics" of COVID-19 cybercrime, including brute-force attacks were up 400%, the number of unsecured remote desktop machines rose by more than 40%, COVID-19-related email scams surged 667% in March, tens of thousands of coronavirus related domains are created daily – and 90% of those new domains are "scammy." It further noted that 530K Zoom accounts were sold on the Dark Web, and a 2000% increase in malicious files with "Zoom" in the name. A 2020 SonicWall cyber threat report cited a 105% spike of ransomware samples.

Lock up sensitive information

Because staff is working from home (WFH), company leaders simply do not know if staff are ignoring best practices, or unsafely storing sensitive information. Therefore, the enterprise must turn to effective plans of action. Briefly, the 411 on the current cyber threat situation revolves around: Personal devices used for work can be hacked in a multitude of ways; the vast majority of hacks don't use malware; unemotional and undaunted by a lack of feeling, AI is a great tool to use, and won't be jeopardized by human error, and now is the time for companies to adopt and integrate much-needed security measures, supported by great company/employee communication, trainings, etc.

The enterprise needs to be concerned. "At home, employees and executives are communicating online with colleagues much more frequently, and they are doing so increasingly on personal devices, personal email accounts, and non-work applications," said Chris Cleveland, founder of AI-powered phishing prevention company Pixm. "This multiplies the entry points attackers have to breach an organization, particularly those that are not protected by corporate email and firewalls."

"Lookout data showed a 24% increase in use of iOS devices in the first 90 days of the pandemic," explained Chris Hazelton, director of security solutions at Lookout. "This equates to several more hours a day of use for many employees." Hazelton added that "more phishing attacks come via personal apps than email. Phishing attacks or malicious payloads delivered by work email are stopped by corporate email gateways, but it is the lack of similar protection for personal mobile apps that creates a significant opportunity for attackers to target remote workers."

Insiders who are also outsiders

It's important to remember that it's not only team leaders and their teams telecommuting, "IT and security stakeholders are themselves more remote than ever from the people they are trying to protect," Cleveland said. “This makes it harder to influence their users toward better cyber hygiene and awareness, particularly for employee training efforts.”

He notes that Q1 saw a 350% increase in phishing attacks, much hinged on impersonating tax-relief efforts by government entities like the IRS or HMRC – unsurprising, because individuals as well as business owners were anxious to claim much-needed benefits.

The psychology of hacking and a fearful remote workforce

The COVID-19 crisis exacerbated existing vulnerabilities, which “are not new, but the pandemic and WFH environment have exacerbated and accelerated them,” he said. “General anxiety around the pandemic, longer work hours and related emotional stress can short circuit people’s short term decision making, which hackers are exploiting with phishing.”

Here’s what hackers want – employee credentials. Cleveland cites it as the No. 1 data-breach vector and said: “Today that is easier than ever as there is an increasing number of accounts employees use to share and access sensitive digital assets. Since most traditional enterprise defense against phishing emails and malicious URLs hinge on the webs’ reputation and threat intelligence, there is a big fat window of time to launch a new attack and steal passwords before an attack is reported and those reputation and intelligence tools start working. This is why 75% of credentials are harvested within the first hour a phishing attack is deployed.”

Hacker tools start with the familiar malwareless phishing, followed by “open-source phishing kits that can phish two-factor authentication codes in real-time,” Cleveland said. “Much more common than that are hackers hijacking the reputation of 3rd party websites, by first breaching them and using them to deliver phishing pages to targets.”

Digital Shadows, a software company, identified an increase of 160% in the number of total cyberattacks in 2020, when compared to 2019, said Ivan Righi, the company’s cyber threat intelligence analyst.

“Spearphishing and account takeover attacks (ATO) remain the most credible threats to remote workers,” Righi said. “Nearly 30% of all remote work incidents since the start of the COVID-19 pandemic were attributed to phishing attacks. A successful phishing attack could give threat actors a foothold on the victim’s network, where they can later move laterally and spread malware, such as ransomware, on critical systems.”

But in addition to personal device security concerns, home equipment may also play a role, said Brandon Hoffman, chief information security officer at Netenrich. “There are some more manual approaches as an initial entry point that remote workers create opportunity for. Some examples in crude weak security on home routers or smart devices attached to the same network. Even in these scenarios, if a manual attack against something like a printer takes place to gain access to the network, at some point malware will likely be delayed against the target machine.”

Safeguards

“Employees have always been on the front lines when it comes to cyberattacks, whether they are targeted at the office or at home,” said Joseph Carson, chief security scientist and advisory chief information security officer at Thycotic, a protection software company. “However, when targeting employees at home, cybercriminals typically had to wait for the employee to return to the office or open a VPN connection to abuse stolen credentials and gain further access to the victim’s employer. With the increase in today’s remote workforce, many organizations have opened persistent connections from employee's home offices, allowing cybercriminals to jump onto those connections and abuse remote access immediately."

"IT security can reduce the risks from such threats by increased cyber security awareness for employees and practicing the principle of least privilege, meaning employee credentials cannot be abused by criminals to gain access to other parts of the organization's network. A strong cyber defense starts with the employee and the ability to detect attacks that start from their home network as well as the ability to reduce those risks with a strong privileged access security solution that can implement a least privilege strategy."

"Non-security incidents can have a substantial knock-on effect within the information security spectrum," weighed in Steve Durbin, managing director of the Information Security Forum, an organization of cyber, information and risk management businesses. "In 2020, the striking example has been the global COVID-19 pandemic, which forced digital change on organizations at high speed and certainly faster than many had dealt with before. It meant that senior IT and security managers have been called on to refocus efforts and help their organization oriented around secure remote working practices. They also had to ensure supply chains remain secure and roll out tailored security awareness campaigns and training, for example to combat the sudden flood of phishing scams related to COVID-19. COVID-19 represents both a crisis and an opportunity. It has accelerated and concentrated forces, such as the move to remote working and adoption of cloud services, that were already in motion. Organizations must be willing to respond to non-information security-related threats if they have a significant impact on the way an organization operates or threaten its technical infrastructure."

Finally, "As well as using digital tools, it's paramount that enterprises stick to high-security standards," Cleveland stressed. An "employee should always follow their employer's advised best practices to avoid being the cause of a costly breach.

At the very minimum, best practices should include using company-issued devices equipped with security controls where possible, VPN usage from personal devices, and training on basic security practices. Companies should implement a disaster recovery and business continuity plan, and purchase cybersecurity liability insurance."

Organizations should take a critical look at "how many employees have access to authorized and confidential material that needs to be kept secure, it's a breach risk. Individuals should consider cybersecurity as a job requirement, and not something left for IT, Cleveland said. "If individuals take responsibility, IT teams can spend less time tending to attacks and more time paving the way towards a remote-ready cybersecurity solution."

Cleveland cited three of what he considers the most common ways to contend with cybersecurity:

- **Communication:** Employees should feel like they have a stake in their company's data security. Good communication should be an organization-wide alignment.
- **Awareness training:** Common, and not entirely super effective, as it was found to reduce phishing clicks by 75%, but it is a start.
- **Install real-time AI applications on the user devices:** "This can augment real-time decision making for end-users to prevent threats that bypass and circumvent the existing corporate security funnel," Cleveland said. "It can also support users in WFH environments. Browser-based AI tools, in particular, can protect users from phishing links delivered outside their corporate email, like LinkedIn, WhatsApp and personal email."

08 Oct 2020

41 8 tips to tighten up your work-from-home network

by Paul Ducklin

https://nakedsecurity.sophos.com/2020/10/08/8-tips-to-tighten-up-your-work-from-home-network/

Every time you hook up a poorly-protected device to your network, you run the risk that crooks will find it, probe it, attack it, exploit it and – if things end badly – use it as a toehold to dig into your digital life.

Criminals who figure out how to commandeer a vulnerable device inside your network can use that device to map out, scan and attack your laptop – the one you're using right now to work from home – as if they were right there beside you.

If you've ever played around with IoT devices, for example, you'll probably know that many of them are based on the Linux kernel and the open source system software that typically forms the core of any Linux distribution.

Indeed, even the tiniest and most stripped-down devices often include not only special-purpose software tailored to that device, but also a host of standard Unix comand line utilities that are the same as, or very similar to, the tools you will find in any penetration tester's toolbox.

For example, a device such as a webcam or smart speaker usually doesn't just contain audio and video processing code.

You'll probably also find:

- **One or more command shells.** Shells such as bash, lash, ash or dash make it easy to run command scripts to automate system management tasks.
- **LAN and wireless configuration programs.** Tools such as ifconfig, ip, iwlist and iwconfig make it straightforward to to map out and configure network settings.
- **Downloader tools.** Programs such as curl and wget can be used used not only for downloading files over the internet, but also for uploading stolen data to outside websites, typically just with a single command.
- **Other scripting software.** You will often find programming tools such as awk, mawk or gawk, a minimalist scripting language that can be used to write internet clients and servers, as well sifting and searching files, all in just a few lines of code.
- **Scheduling tools.** Program such as cron or an equivalent make it easy to schedule programs to run at regular times even when no one is logged in, for example to watch out for computers being connected to the network and sending back a notification message.
- **Remote access and encryption tools.** Many IoT devices include both SSH client and server software such as ssh, sshd or dropbear. These give crooks a way to create secret, encrypted network "tunnels" into and out of your network using software that's already there.

- **Network and account passwords.** Your Wi-Fi password may very well be stored in a plaintext file on the device, such as /etc/wpa_supplicant.conf. Password or authentication tokens for any accounts that the device is hooked up to may be lying around for the taking, too.

Generally speaking, the closer the crooks get to your computer on the internet, the more aggressively they can attack it – and the next best thing to being on your computer already is to be right next door on the same network with their favourite hacking tools preinstalled.

What to do?

By now, it might sound as though you need an enormous range of skills just to figure out where to start, let alone where to finish, in securing your own network to be robust enough for WFH. (ICYMI, that's short for working from home.)

The good news is that you don't need the combined practical experience of an IT manager, a tech support guru, a penetration tester and a network engineer.

We've come up with eight questions you can ask yourself about devices on your home network, and about the setup of your network, that will help you run a tighter WFH ship.

Think of it as going through your very own Cybersecurity Awareness Month at home:

- **Step 1. Do I actually need this device online?** If not, consider removing it from your network. Or if you don't need it listening in or activated all the time, consider powering it down when you aren't using it. (Unplugging it from the wall socket is often all you need to do.)

- **Step 2. Do I know how to update it?** If not, find out how. If the vendor can't reassure you about security updates, consider switching products to a vendor that does (and see step 1).

- **Step 3. Do I know how to configure it?** Make sure you know what security settings are available, what they are for, and how to set them up (and see step 2).

- **Have I changed any risky default settings?** Many IoT devices come with remote troubleshooting features turned on, which crooks may be able to abuse. They also often arrive with default passwords set, which the crooks will definitely know. Some routers ship with Universal Plug and Play enabled, which can expose the inside of your network by mistake. Check and change defaults before you make the device live (and see steps 2 and 3).

- **Step 5. How much am I sharing?** If the device is hooked up to an online service, familiarise yourself with how much data the device is sharing, and how often. You may be happy to share some data, but never feel squeezed into turning all the options "to the max" (and see steps 3 and 4).

- **Step 6. Can I "divide and conquer" my network?** Some home routers let you split your Wi-Fi into two networks that can be managed separately. This is useful if you are working from home because it means you can put your home IoT devices on a "guest" network and your work computers such as laptops on another (and see steps 1, 2, 3, 4 and 5).

- **Step 7. Can I turn on "client isolation"?** Some home routers have an option known as client isolation that shields devices on the network from each other. This reduces the risk of a security hole in one device being used to attack other computers "from inside" (and see steps 1, 2, 3, 4, 5, and 6).

- **Step 8. Do I know whom to turn to if there's a problem?** If your work has an IT department or offers access to tech support, make sure you know where to report anything suspicious. Ask them what information they are likely to need and provide it at the outset, in order to speed up the process.

By the way, if you're an IT department looking after remote workers, make it easy for your less-technical colleagues to reach out for cybersecurity advice, or to report suspicious activity, and take the attitude that there's no such thing as a stupid question, only a stupid answer.

In our experience, most employees are ready and willing to do the right thing when it comes to cybersecurity – after all, if they get hacked while WFH then their own digital life is at risk along with the company's.

Set up an internal email or telephone reporting line where users can easily and efficiently possible attacks and get the whole company to be the eyes and ears of the security team!

42 Generating photons for communication in a quantum computing system

by Michaela Jarvis

https://phys.org/news/2020-10-photons-quantum.html?

MIT researchers using superconducting quantum bits connected to a microwave transmission line have shown how the qubits can generate on demand the photons, or particles of light, necessary for communication between quantum processors.

The advance is an important step toward achieving the interconnections that would allow a modular quantum computing system to perform operations at rates exponentially faster than classical computers can achieve.

"Modular quantum computing is one technique for reaching quantum computation at scale by sharing the workload over multiple processing nodes," says Bharath Kannan, MIT graduate fellow and first author of a paper on this topic published today in Science Advances. "These nodes, however, are generally not co-located, so we need to be able to communicate quantum information between distant locations."

In classical computers, wires are used to route information back and forth through a processor during computation. In a quantum computer, the information itself is quantum mechanical and fragile, requiring new strategies to simultaneously process and communicate information.

"Superconducting qubits are a leading technology today, but they generally support only local interactions (nearest-neighbor or qubits very close by). The question is how to connect to qubits that are at distant locations," says William Oliver, an associate professor of electrical engineering and computer science, MIT Lincoln Laboratory fellow, director of the Center for Quantum Engineering, and associate director of the Research Laboratory of Electronics. "We need quantum interconnects, ideally based on microwave waveguides that can guide quantum information from one location to another."

That communication can occur via the microwave transmission line, or waveguide, as the excitations stored in the qubits generate photon pairs, which are emitted into the waveguide and then travel to two distant processing nodes. The identical photons are said to be "entangled," acting as one system. As they travel to distant processing nodes, they can distribute that entanglement throughout a quantum network.

"We generate the entangled photons on demand using the qubits and then release the entangled state to the waveguide with very high efficiency, essentially unity," says Oliver.

The research reported in the Science Advances paper utilizes a relatively simple technique, Kannan says.

"Our work presents a new architecture for generating photons that are spatially entangled in a very simple manner, using only a waveguide and a few qubits, which act as the photonic emitters," says Kannan. "The entanglement between the photons can then be transferred into the processors for use in quantum communication or interconnection protocols."

While the researchers said they have not yet implemented those communication protocols, their ongoing research is aimed in that direction.

"We did not yet perform the communication between processors in this work, but rather showed how we can generate photons that are useful for quantum communication and interconnection," Kannan says.

Previous work by Kannan, Oliver, and colleagues introduced a waveguide quantum electrodynamics architecture using superconducting qubits that are essentially a type of artificial giant atom. That research demonstrated how such an architecture can perform low-error quantum computation and share quantum information between processors. This is accomplished by adjusting the frequency of the qubits to tune the qubit-waveguide interaction strength so the fragile qubits can be protected from waveguide-induced decoherence to perform high-fidelity qubit operations, and then readjusting the qubit frequency so the qubits are able to release their quantum information into the waveguide in the form of photons.

This paper presented the photon generation ability of the waveguide quantum electrodynamics architecture, showing that the qubits can be used as quantum emitters for the waveguide. The researchers demonstrated that quantum interference between the photons emitted into the waveguide generates entangled, itinerant photons that travel in opposite directions and can be used for long-distance communication between quantum processors.

Generating spatially entangled photons in optical systems is typically accomplished using spontaneous parametric down-conversion and photodetectors, but the generated entanglement achieved that way is generally random and therefore less useful in enabling on-demand communication of quantum information in a distributed system.

"Modularity is a key concept of any extensible system," says Oliver. "Our goal here is to demonstrate the elements of quantum interconnects that should be useful in future quantum processors."

07 Oct 2020

43 Aliro Quantum Introduces Its First Software Products for Computing and Networking

https://quantumcomputingreport.com/aliro-quantum-introduces-its-first-software-products-for-computing-and-networking/

Aliro Quantum, a quantum software company spun out of spun out of Harvard's Quantum Information Science Lab in 2019, has introduced its first two products. The first is called **Aliro Q.Compute (AQC)** and is a development platform that will take quantum programs written in QASM, pyQuil, or other quantum languages and optimize them to run on different hardware platforms. Aliro currently supports hardware from IBM, Honeywell, Rigetti, AQT, and they are working to add others. The software will create noise models for the various hardware platforms and then develop optimizations a both the gate level and the pulse level to run a user's program with the best performance and accuracy. By supporting multiple hardware backends, the Aliro software can also guide a user to select the best hardware platform for their particular problem.

The second software product is called **Aliro Q.Network (AQN)** is quite unique. It is a quantum network simulator that allows one to design and configure a quantum network. The AQN allows a user to select a topology, look at component fidelities, configure devices, simulate noise sources, compare protocols, and more. The output of the AQN will provide the user with estimates of the network performance, resources estimates, and cost. Although there are a lot of quantum software companies out there, we do not know of anyone that is tackling the quantum networking issues in the way that Aliro is.

When many people think about a quantum internet, they often think of QKD networks which allow one to send and receive data between two classical computers in a way that cannot be broken with a future large quantum computer running Shor's algorithm. However, one trend we see coming to quantum computing is the notion of using multiprocessing architectures to solve much larger quantum programs. Rather than hardware companies developing a single individual processor that contains 1 million qubits, we expect that in a few years, some of them will be providing multiprocessing systems that will have perhaps a thousand or so qubits in a single processor, but then replicate those processors 100 or more times to create systems with 10's of thousands or 100's of thousands of qubits. The individual processors will be networked with a form of quantum internet that will exchange entangled photons with the other processors and be programmed together to run a much larger quantum application program. Although the multiprocessors may be located in different cities, they may also be clustered together within a quantum data center with an average node-to-node distance of 1 or 2 meters.

Aliro has received grants from the U.S. Air Force Research Laboratory (AFRL) and is working with them on various use cases. Both software programs are currently in beta test with selected customers.

44 New Algorithm Helps Quantum Computers Skip Past the Time Limits Imposed by Decoherence

by Matt Swayne

https://thequantumdaily.com/2020/10/07/new-algorithm-helps-quantum-computers-skip-past-the-time-limits-imposed-by-decoherence/

A new algorithm that fast forwards simulations could bring greater use ability to current and near-term quantum computers, opening the way for applications to run past strict time limits that hamper many quantum calculations, according to a news release from Los Alamos National Laboratory.

"Quantum computers have a limited time to perform calculations before their useful quantum nature, which we call coherence, breaks down," said Andrew Sornborger of the Computer, Computational, and Statistical Sciences division at Los Alamos National Laboratory, and senior author on a paper announcing the research. "With a new algorithm we have developed and tested, we will be able to fast forward quantum simulations to solve problems that were previously out of reach."

Computers built of quantum components, known as qubits, can potentially solve extremely difficult problems that exceed the capabilities of even the most powerful modern supercomputers. Applications include faster analysis of large data sets, drug development, and unraveling the mysteries of superconductivity, to name a few of the possibilities that could lead to major technological and scientific breakthroughs in the near future.

Recent experiments have demonstrated the potential for quantum computers to solve problems in seconds that would take the best conventional computer millennia to complete. The challenge remains, however, to ensure a quantum computer can run meaningful simulations before quantum coherence breaks down.

“We use machine learning to create a quantum circuit that can approximate a large number of quantum simulation operations all at once,” said Sornborger. “The result is a quantum simulator that replaces a sequence of calculations with a single, rapid operation that can complete before quantum coherence breaks down.”

The Variational Fast Forwarding (VFF) algorithm that the Los Alamos researchers developed is a hybrid combining aspects of classical and quantum computing. Although well-established theorems exclude the potential of general fast forwarding with absolute fidelity for arbitrary quantum simulations, the researchers get around the problem by tolerating small calculation errors for intermediate times in order to provide useful, if slightly imperfect, predictions.

In principle, the approach allows scientists to quantum-mechanically simulate a system for as long as they like. Practically speaking, the errors that build up as simulation times increase limits potential calculations. Still, the algorithm allows simulations far beyond the time scales that quantum computers can achieve without the VFF algorithm.

One quirk of the process is that it takes twice as many qubits to fast forward a calculation than would make up the quantum computer being fast forwarded. In the newly published paper, for example, the research group confirmed their approach by implementing a VFF algorithm on a two qubit computer to fast forward the calculations that would be performed in a one qubit quantum simulation.

In future work, the Los Alamos researchers plan to explore the limits of the VFF algorithm by increasing the number of qubits they fast forward, and checking the extent to which they can fast forward systems. The research was published September 18, 2020 in the journal npj Quantum Information.

The research was supported with funding from the Los Alamos National Laboratory Information Science & Technology Institute, Department of Energy Advanced Scientific Computing Beyond Moore’s Law program, and the Los Alamos National Laboratory Directed Research and Development program.

06 Oct 2020

45 The road to Eindhoven’s hybrid quantum computer

by Barry Fitzgerald

https://www.tue.nl/en/our-university/departments/biomedical-engineering/the-department/news/news-overview/06-10-2020-the-road-to-eindhovens-hybrid-quantum-computer/

The need to continue developments in quantum computers is an indicator of the future importance of these computational platforms. In 2020, the Dutch government committed €23.5 million to quantum innovation, an investment coordinated by QuantumDeltaNL. Part of this funding will be used to build a hybrid quantum computer – a device consisting of both classical and quantum computing technologies – at Eindhoven University of Technology by 2024, which will be accessible 24/7 for scientific computations.

Physicist Servaas Kokkelmans explains the challenges and quantum enemies that must be overcome to create this unique computer.

Our daily reliance on computers is self-evident. We use computers to send e-mails, order furniture, watch our favourite Marvel films, and to video chat with people around the world.

Computers have also led to once unimaginable possibilities in society. In industry, computers have enhanced and optimized manufacturing processes, created new product lines, and decreased the need for piles of tedious paperwork.

In the world of science and engineering, computers have helped instigate new disciplines such as numerical simulations, bio-informatics, and computational design. Scientific advances in many disciplines would have been impossible without the computer.

QUANTUM ASSISTANCE

Nonetheless, even the current generation of supercomputers face insurmountable hurdles in solving problems in certain disciplines such as medicine, quantum chemistry, and material science.

Fortunately, the quantum computing age is gaining significant traction, with researchers such as Associate Professor Servaas Kokkelmans, director and one of the main proponents of quantum technologies at QT/e – the Center for Quantum Materials and Technology Eindhoven – which is TU/e's dedicated research center for quantum technologies, working on quantum technologies.

He is working towards a future where quantum computers can have a similar impact on society as the classical computer did in the past. "Quantum researchers all want to push quantum technology, and at Eindhoven, we are striving to create a very unique interpretation of the quantum computer – a hybrid quantum computer – a computer that combines classical and quantum computing technologies", says Kokkelmans. '"We've cracked the classical part of this problem, but the quantum part still needs work."

Building a successful quantum computer is fraught with challenges. First, a design must be envisaged, evaluated, and revised. Once a quantum computer design is theoretically confirmed the next step is actually building it. This requires particular materials that must be stored under specific conditions, and as you'll see this can be quite problematic.

But before delving into the challenges associated with building quantum computers, let's meet the fundamental component of a quantum computer – the qubit.

REPLACING "1 OR 0" WITH "1 AND 0"

Classical computers typically store information as bits that can have one of two values – 1 or 0. In other words, they store information in binary format. Every day, you change the information in the bits of computer memory, microprocessors, graphics cards, and magnetic storage devices. Your life really is just the sum of changing bits.

In quantum computers, the classical bits are replaced by quantum bits or qubits. Examples of qubits include photons (with horizontal or vertical polarization) or electrons (with spin-up or spin-down).

Thanks to the wonders of quantum mechanics, a qubit can store both a 1 and 0 state at the same time, and all other states in between. This counter-intuitive quantum behavior is known as superposition, and it means that a group of qubits can theoretically store all programmable values at the same time.

In magnetic storage devices or semiconductor materials in classical computers, bits are represented as tiny bar magnets or a memory cell consisting of one or more transistors respectively. For magnetic materials, the tiny bar magnets can point up or down, with these states representing 1 or 0.

On the other hand, to make qubits, you need to look to the atomic scale, more specifically the electrons that orbit the nucleus of atoms.

"Atoms are the perfect qubits because they are all the same. In addition, they provide us with access to two definite states – spin-up and spin-down – associated with any electron that orbits the nucleus," says Kokkelmans. "However, only certain atoms can be used as qubits, and to ensure they remain stable for a hybrid quantum computer, these atoms also need to be ultracold."

COOLING THE RIGHT QUBITS

While all atoms have electrons, only certain atoms are suitable to be used as qubits. With one electron orbiting its nucleus, hydrogen might seem like the perfect qubit. Nothing could be further from the truth. "One reason that hydrogen is not used is that it is really hard to cool and trap, and many people have tried to this in the laboratory," states Kokkelmans.

Appropriate qubit atoms lie elsewhere on the Periodic Table in the form of rubidium (Rb) and strontium (Sr), which can be found in the first and second column of the Periodic Table respectively. Kokkelmans and his colleagues have a lot of experience in working with rubidium for quantum devices but it's not the perfect qubit atom. "Rubidium is a heavy atom and easy to cool, but there are issues with fidelity – which is a measure of how close your quantum system is to the state that you want it to be in."

The alternative is to use strontium atoms. "Strontium atoms are more difficult to handle or cool in comparison to rubidium atoms, but they have better fidelity than rubidium atoms. For this reason, we may seek to change the atom and build our hybrid quantum computer at TU/e using ultracold, strontium atoms," says Kokkelmans.

Counter-intuitively, lasers are used to ultracool atoms to temperatures in the microkelvin range, and Kokkelmans has a nice analogy to explain the use of lasers in cooling. "Imagine an atom as a football, and that the laser emits photons that can be seen as small ping-pong balls. When we shine lasers from a number of different directions on an atom, the photons hit the atom from all directions. As a result, the atom is slowed down in all directions and then confined to an ultracold optical trap."

QUANTUM DECOHERENCE – THE ENEMY OF THE QUANTUM COMPUTER

In addition to cooling, lasers are also used to excite atoms to so-called Rydberg states, which is needed to promote interactions between neighboring qubits.

In a crystalline solid, atoms are very close to each other and they can feel or interact with each other all of the time. This arrangement would not work for a collection of qubit atoms, as it would then be almost impossible to isolate the individual atoms using lasers.

As part of their work, Kokkelmans and his collaborators create artificial crystals where the atoms are arranged in a regular lattice using optical tweezers – another term for a focused laser used to hold an atom, but the atoms are much further apart than in a normal crystal. They use a special trick to get the atoms to feel each other. "We excite the atoms to Rydberg states. This allows us to keep the atoms far enough apart so that they are isolated, but as they are excited, that they can still feel each other," notes Kokkelmans.

The stability of the quantum state of the ultracold qubits can be affected by many factors. External heat or vibrations can perturb the ultracold qubits, while the reliability of the lasers used to hold and manipulate the atoms can have a negative effect. This can lead to quantum decoherence of the qubits, which means that the superposition and entanglement of the qubit quantum states starts to vanish.

“You can look at quantum decoherence as the enemy of the quantum computer, and this is something we really have to worry about,” says Kokkelmans. In principle, it is possible to correct for these effects with quantum error correction, where additional qubits are used to store past quantum states.

However, the thresholds for applying these techniques are quite high, and researchers worldwide are far from implementing them. This is typical of the current era of quantum computing, which is known as the Noisy Intermediate Scale Quantum (NISQ) regime. This refers to qubit devices subjected to decoherence without error correction that are on the threshold of demonstrating quantum speedup with respect to classical computers.

HYBRID QUANTUM COMPUTER – BEST OF BOTH WORLDS

Once a reliable and stable method for storing ultracold strontium atoms is developed and proper single-qubit addressing is included, Kokkelmans and his colleagues from QT/e and QuantumDeltaNL will have their quantum qubit device with high fidelity qubits, although without quantum error correction. They can then take the next step of combining this device with a classical computer to make a hybrid quantum computer.

“A hybrid quantum computer exploits the best of both worlds as it seeks to have the best parts of a quantum device and a classical supercomputer work together,” says Kokkelmans. In a hybrid quantum computer, the quantum device will act as a quantum co-processor that works with a classical device, which will include circuits for control and pre- and post-processing. Moreover, the algorithms that run on a hybrid quantum computer are more robust towards decoherence, and therefore reduce the need for quantum error correction.

But why build a hybrid quantum computer in the first place? Well, it all comes down to application.

“Classical supercomputers are used extensively to do chemical calculations. Perhaps 20% of supercomputer time worldwide is devoted to these calculations. In many cases quantum calculations are required, and that’s where the quantum computer comes to the fore,” says Kokkelmans. “In effect, a hybrid quantum computer could carry out chemical calculations in a more natural and faster manner than a classical supercomputer.”

PLANS IN PLACE

The plans are very much in place for Eindhoven’s hybrid quantum computer. “We are busy redesigning our setup using qubits based on strontium atoms, and we aim to be fully operational by 2024. Then we will connect our device to the Quantum Inspire network, which means that anyone can run quantum code on the hybrid device,” notes Kokkelmans.

The hybrid quantum computer will be open source and available for anyone to use. People can decide what type of calculation that they want to run on Quantum Inspire and on which quantum platform. For instance, researchers can opt to run chemical or material science calculations on the Eindhoven quantum infrastructure.

While some may anticipate that quantum computers will eventually succeed classical computers, the truth is these computational systems look destined to complement each other in future computational infrastructure such as hybrid quantum computers.

Thanks to research initiatives such as QT/e and their collaboration with the other national research institutes of QuantumDeltaNL, Servaas Kokkelmans and his collaborators look set to be part of the quantum computing revolution.

The challenges and quantum enemies standing in the way of Eindhoven's hybrid quantum computer look set to be vanquished.

46 EU's top court limits government spying on citizens' mobile and internet data

by Sam Shead

https://www.cnbc.com/2020/10/06/ecj-limits-government-spying-on-citizens-mobile-and-internet-data-.html

The top court in the European Union has delivered another blow to governments seeking to keep tabs on citizens through controversial spying techniques.

The European Court of Justice (ECJ), the EU's highest legal authority, ruled Tuesday that member states cannot collect mass mobile and internet data on citizens.

Forcing internet and phone operators to carry out the "general and indiscriminate transmission or retention of traffic data and location data" is against EU law, the court explained in its ruling.

"However, in situations where a member state is facing a serious threat to national security that proves to be genuine and present or foreseeable, that member state may derogate from the obligation to ensure the confidentiality of data relating to electronic communications," it continues.

Even in these emergency scenarios, there are rules that must be adhered to.

"Such an interference with fundamental rights must be accompanied by effective safeguards and be reviewed by a court or by an independent administrative authority," the court said.

The ruling, which has been eagerly anticipated by civil rights campaigners, is in response to several cases brought about by Privacy International and La Quadrature du Net.

The campaign groups argued that surveillance practices in the U.K., France and Belgium go too far and violate fundamental human rights. The groups specifically took issue with the U.K.'s Investigatory Powers Act, a 2015 French decree related to specialized intelligence services, and a Belgian law on collection and retention of communications data that was introduced in 2016.

"Today's judgement reinforces the rule of law in the EU," said Caroline Wilson Palow, legal director of Privacy International, in a statement. "In these turbulent times, it serves as a reminder that no government should be above the law. Democratic societies must place limits and controls on the surveillance powers of our police and intelligence agencies."

Palow added: "While the Police and intelligence agencies play a very important role in keeping us safe, they must do so in line with certain safeguards to prevent abuses of their very considerable power. They should focus on providing us with effective, targeted surveillance systems that protect both our security and our fundamental rights."

Opinion from EU court advisor

The ruling comes after an advisor to the ECJ argued that the surveillance practices in the U.K, France and Belgium breached EU laws.

Advocate General Manuel Campos Sanchez-Bordona said in January that EU law prohibits governments from forcing private companies to engage in bulk indiscriminate surveillance.

He said it applies to all situations where governments force telecommunications companies to participate in mass surveillance programs.

The ECJ ruling is the latest in a string of cases trying to limit the powers of governments to keep tabs on citizens.

In July, the ECJ ruled that U.S. national security laws don't protect EU citizens' privacy.

The court restricted how U.S. firms could send European user data to the U.S. after concluding EU citizens had no effective way to challenge American government surveillance. U.S. agencies such as the NSA can theoretically ask internet companies like Facebook and Google to hand over data on an EU citizen and that EU citizen would be none-the-wiser.

The decision came after Austrian privacy activist Max Schrems filed a law suit in light of the Edward Snowden revelations arguing that U.S. law did not offer sufficient protection against surveillance by public authorities. Schrems raised the complaint against Facebook which, like many other firms, was transferring his and other user data to the U.S.

47 A new interpretation of quantum mechanics suggests that reality does not depend on the person measuring it

by Aalto University

https://phys.org/news/2020-10-quantum-mechanics-reality-person.html

Quantum mechanics arose in the 1920s, and since then scientists have disagreed on how best to interpret it. Many interpretations, including the Copenhagen interpretation presented by Niels Bohr and Werner Heisenberg, and in particular, von Neumann-Wigner interpretation, state that the consciousness of the person conducting the test affects its result. On the other hand, Karl Popper and Albert Einstein thought that an objective reality exists. Erwin Schrödinger put forward the famous thought experiment involving the fate of an unfortunate cat that aimed to describe the imperfections of quantum mechanics.

In their most recent article, Finnish civil servants Jussi Lindgren and Jukka Liukkonen, who study quantum mechanics in their free time, take a look at the uncertainty principle that was developed by Heisenberg in 1927. According to the traditional interpretation of the principle, location and momentum cannot be determined simultaneously to an arbitrary degree of precision, as the person conducting the measurement always affects the values.

However, in their study Lindgren and Liukkonen concluded that the correlation between a location and momentum, i.e., their relationship, is fixed. In other words, reality is an object that does not depend on the person measuring it. Lindgren and Liukkonen utilized stochastic dynamic optimization in their study. In their theory's frame of reference, Heisenberg's uncertainty principle is a manifestation of thermodynamic equilibrium, in which correlations of random variables do not vanish.

“The results suggest that there is no logical reason for the results to be dependent on the person conducting the measurement. According to our study, there is nothing that suggests that the consciousness of the person would disturb the results or create a certain result or reality,” says Jussi Lindgren.

This interpretation supports such interpretations of quantum mechanics that support classical scientific principles.

“The interpretation is objective and realistic, and at the same time as simple as possible. We like clarity and prefer to remove all mysticism,” says Liukkonen.

The researchers published their last article in December 2019, which also utilized mathematical analysis as a tool to explain quantum mechanics. The method they used was stochastic optimal control theory, which has been used to solve such challenges as how to send a rocket from the Earth to the Moon.

Following Occam’s razor, the law of parsimony named after William of Ockham, the researchers have now chosen the simplest explanation from those that fit.

“We study quantum mechanics as a statistical theory. The mathematical tool is clear, but some might think it is a boring one. But is an explanation really an explanation, if it’s a vague one?” asks Lindgren.

48 Quantum simulation beyond the coherence time

https://www.swissquantumhub.com/quantum-simulation-beyond-the-coherence-time/

Iterative approaches to Quantum Simulation (QS) are restricted to simulation times less than the coherence time of the Quantum Computer (QC), which limits their utility in the near term.

Researchers at Los Alamos have developed is a hybrid combining aspects of classical and quantum computing. Although well-established theorems exclude the potential of general fast forwarding with absolute fidelity for arbitrary quantum simulations, the researchers get around the problem by tolerating small calculation errors for intermediate times in order to provide useful, if slightly imperfect, predictions.

The team has proposed a hybrid quantum-classical algorithm, called **Variational Fast Forwarding** (VFF), for decreasing the quantum circuit depth of QSs. VFF seeks an approximate diagonalization of a short-time simulation to enable longer-time simulations using a constant number of gates.

Their error analysis provided two results:

(i) the simulation error of VFF scales at worst linearly in the fast-forwarded simulation time, and

(ii) their cost function’s operational meaning as an upper bound on average-case simulation error provides a natural termination condition for VFF.

The researchers implemented VFF for the Hubbard, Ising, and Heisenberg models on a simulator. In addition, they also implemented VFF on Rigetti’s Quantum Computers to demonstrate simulation beyond the coherence time.

Finally, they showed how to estimate energy eigenvalues using VFF.

05 Oct 2020

49 Quantum computing: Photon startup lights up the future of computers and cryptography

by Daphne Leprince-Ringuet

https://www.zdnet.com/google-amp/article/quantum-computing-photon-startup-lights-up-the-future-of-computers-and-cryptography/

UK startup Nu Quantum is breaking new ground in the quantum photonics space.

A fast-growing UK startup is quietly making strides in the promising field of quantum photonics. Cambridge-based company Nu Quantum is building devices that can emit and detect quantum particles of light, called single photons. With a freshly secured £2.1 million ($2.71 million) seed investment, these devices could one day underpin sophisticated quantum photonic systems, for applications ranging from quantum communications to quantum computing.

The company is developing high-performance light-emitting and light-detecting components, which operate at the single-photon level and at ambient temperature, and is building a business based on the combination of quantum optics, semiconductor photonics, and information theory, spun out of the University of Cambridge after eight years of research at the Cavendish Laboratory.

“Any quantum photonic system will start with a source of single photons, and end with a detector of single photons,” Carmen Palacios-Berraquero, the CEO of Nu Quantum, tells ZDNet. “These technologies are different things, but we are bringing them together as two ends of a system. Being able to controllably do that is our main focus.”

As Palacios-Berraquero stresses, even generating single quantum particles of light is very technically demanding.

In fact, even the few quantum computers that exist today, which were designed by companies such as Google and IBM, rely on the quantum states of matter, rather than light. In other words, the superconducting qubits that can be found in those tech giants’ devices rely on electrons, not photons.

Yet the superconducting qubits found in current quantum computers are, famously, very unstable. The devices have to operate in temperatures colder than those found in deep space to function, because thermal vibrations can cause qubits to fall from their quantum state. On top of impracticality, this also means that it is a huge challenge to scale up the number of qubits in the computer.

A photonic quantum computer could have huge advantages over its matter-based counterpart. Photons are much less prone to interact with their environment, which means they can retain their quantum state for much longer and over long distances. A photonic quantum computer could, in theory, operate at room temperature – and as a result, scale up much faster.

The whole challenge comes from creating the first quantum photon, explains Palacios-Berraquero. “Being able to emit one photon at a time is a ground-breaking achievement. In fact, it has become the Holy Grail of quantum optics.”

“But I worked on generating single photons for my PhD. That’s the IP I brought to the table.”

Combined with improved technologies in the fields of nanoscale semi-conductor fabrication, Palacios-Berraquero and her team set off to crack the single-photon generation problem.

Nu Quantum’s products come in the form of two little boxes: the first one generates the single photons that can be used to build quantum systems for various applications, and the other measures the quantum signals emitted by the first one. The technology, maintains the startup CEO, is bringing quantum one step closer to commercialization and adoption.

“Between the source and the detector of single photons, many things can happen, from the simplest to the most complex,” explains Palacios-Berraquero. “The most complex one being a photonic quantum computer, in which you have thousands of photons on one side and thousands of detectors on the other. And in the middle, of course, you have gates, and entanglement, and . . . and, and and. But that’s the most complex example.”

A photonic quantum computer is still a very long-term ambition of the startup CEO. A simpler application, which Nu Quantum is already working on delivering commercially with the UK’s National Physical Laboratory, is quantum random number generation – a technology that can significantly boost the security of cryptographic keys that secure data.

The keys that are currently used to encrypt the data exchanged between two parties are generated thanks to classical algorithms. Classical computing is deterministic: a given input will always produce the same output, meaning that complete randomness is fundamentally impossible. As a result, classical algorithms are predictable to an extent. In cryptography, this means that security keys can be cracked fairly easily, given sufficient computing power.

Not so much with quantum. A fundamental property of quantum photons is that they behave randomly: for example, if a single photon is sent down a path that separates in two ways, there is no way of knowing deterministically which way the particle will choose to go through.

The technology that Nu Quantum is developing with the National Physical Laboratory, therefore, consists of a source of single photons, two detectors, and a two-way path linking the three devices. “If we say the right detector is a 1, and the left detector is a 0, you end up with a string of numbers that’s totally random,” says Palacios-Berraquero. “The more random, the more unpredictable the key is, and the more secure the encryption.”

Nu Quantum is now focusing on commercializing quantum random number generation, but the objective is to build up systems that are increasingly complex as the technology improves. Palacios-Berraquero expects that in four or five years, the company will be able to start focusing on the next step.

One day, she hopes, Nu Quantum’s devices could be used to connect quantum devices in a quantum internet – a decade-long project contemplated by scientists in the US, the EU, and China, which would tap the laws of quantum mechanics to almost literally teleport some quantum information from one quantum device to the next. Doing so is likely to require single photons to be generated and distributed between senders and receivers, because of the light particles’ capacity to travel longer distances.

In the shorter term, the startup will be focusing on investing the seed money it has just raised. On the radar, is a brand-new lab and headquarters in Cambridge, and tripling the size of the team with a recruitment drive for scientists, product team members and business functions.

04 Oct 2020

50 Is Quantum Cryptography The Solution to Internet Security?

by Naveen Joshi

https://www.bbntimes.com/technology/is-quantum-cryptography-the-solution-to-internet-security

Quantum cryptography might hold the key to internet security as computers have become relatively faster and quicker at decrypting data.

Encryption today, as we know, is based on numbers that are hard to factorize. However, as we near the quantum computing breakthrough, these encryption methods will no longer be secure. It will become relatively easy for hackers to decrypt data in minutes with the help of quantum computing. Even highly secure technologies are vulnerable to the misuse of quantum computing. However, quantum cryptography can help make your data much more secure so that only the sender and the receiver can access it.

So, What Exactly is Quantum Cryptography?

In classical cryptography, the encrypted message is shared between the sender and the recipient in the form keys of a few bits length. Typically the 128-bit encryption method is used for encrypting messages. Breaking the 128-bit encryption key is hard on conventional computers due to a large number of possible keys. A 128-bit key has 2^{128} possible combinations to decrypt the data contained. However, with quantum computing, the task of deciphering a 128-bit task becomes relatively easy due to the speed capabilities of quantum computing. Quantum cryptography, by extension, simply uses the principles of quantum mechanics to encrypt data and transmit it in a way that cannot be hacked.

How Does Quantum Cryptography Work?

In quantum physics, the light waves are transferred as photons. The photons can be polarized, either rectilinear or diagonal. The polarization modes are used to map the binary values of 0 and 1, and each photon carries one qubit of information. But unlike classical cryptography, the photon can be either 1 or 0 based on the polarization mode used. A sender can suggest a key by sending randomly polarized photons to the recipient. To decrypt the key, the recipient must measure the polarization by passing it through the correct filter, i.e. rectilinear or diagonal. If a hacker tries to intercept the process, the recipient comes to know of the attack and can ask the sender to cancel the data transmission. The sender then has to send a new stream of randomly polarized photons for the receiver to decrypt. Thus, quantum cryptography makes hacking into a quantum encrypted data much more difficult as compared to classical cryptography.

Benefits of Quantum Cryptography

The following are some of the major benefits of quantum cryptography:

- Provides security based on the fundamental laws of physics
- Virtually impossible to hack
- Simple to use
- Dependence on fewer resources for maintenance
- Capable of detecting hacking attempts in real-time
- Continuously improving in performance, providing better security features by the day

Drawbacks of Quantum Cryptography

Although quantum cryptography can provide a better security layer than conventional cryptography, it is not without its limitations. Some of which include:

- There is a possibility of a change in the polarization of photons
- It lacks features such as a digital signature

The current cybersecurity threats call for strong automated security measures. Although quantum cryptography offers solutions against security threats, the technology isn't completely reliable. A hybrid solution of classical cryptography and quantum cryptography might provide the best defense against cyberattacks, till we perfect the quantum cryptography technology.

51 The Quantum Internet Will Blow Your Mind. Here's What It Will Look Like

by Dan Hurley

https://www.discovermagazine.com/technology/the-quantum-internet-will-blow-your-mind-heres-what-it-will-look-like

Call it the quantum Garden of Eden. Fifty or so miles east of New York City, on the campus of Brookhaven National Laboratory, Eden Figueroa is one of the world's pioneering gardeners planting the seeds of a quantum internet. Capable of sending enormous amounts of data over vast distances, it would work not just faster than the current internet but faster than the speed of light – instantaneously, in fact, like the teleportation of Mr. Spock and Captain Kirk in Star Trek.

Sitting in Brookhaven's light-filled cafeteria, his shoulder-length black hair fighting to free itself from the clutches of a ponytail, Figueroa – a Mexico native who is an associate professor at Stony Brook University – tries to explain how it will work. He grabs hold of two plastic coffee cup lids, a saltshaker, a pepper shaker and a small cup of water, and begins moving them around on the lunch table like a magician with cards.

"I'm going to have a detector here and a detector here," he says, pointing to the two lids. "Now there are many possibilities. Either those two go in here" – he points to the saltshaker – "or the two go in there," nodding at the cup of water. "And then depending on what happened there, that will be the state," he says, holding up the black pepper shaker, "that I'm preparing here."

Got that? Me neither. But don't worry. Only a few hundred or so physicists in the U.S., Europe and China really comprehend how to exploit some of the weirdest, most far-out aspects of quantum physics. In this strange arena, objects can exist in two or more states at the same time, called superpositions; they can interact with each other instantly over long distances; they can flash in and out of existence. Scientists like Figueroa want to harness that bizarre behavior and turn it into a functioning, new-age internet – one, they say, that will be ironclad for sending secure messages, impervious to hacking.

Already, Figueroa says his group has transmitted what he called "polarization states" between the Stony Brook and Brookhaven campuses using fiber infrastructure, adding up to 85 miles. Kerstin Kleese van Dam, director of Brookhaven Lab's Computational Science Initiative, says it is "one of the largest quantum networks in the world, and the longest in the United States."

Next, Figueroa hopes to teleport his quantum-based messages through the air, across Long Island Sound, to Yale University in Connecticut. Then he wants to go 50 miles east, using existing fiber-optic cables to connect with Long Island and Manhattan.

Kleese Van Dam says that although other groups in Europe and China have more funding and have been working much longer on the technology, in the U.S. "[Figueroa] is leading when it comes to having the knowledge and the equipment necessary to put together a quantum network in the next year or two."

David Awschalom, a legend in the field who is a professor of spintronics and quantum information at the University of Chicago's Pritzker School of Molecular Engineering and director of the Chicago Quantum Exchange, calls Figueroa's work "a fantastic project being done very thoughtfully and very well. I'm always cautious about saying something is the biggest or fastest," he says. "It's a worldwide effort right now in building prototype quantum networks as the next step toward building a quantum internet." Other efforts to build quantum networks, he says, are underway in Japan, the U.K., the Netherlands and China – not to mention his own group's project in Chicago.

U.S. efforts have lately been given a boost by the U.S. Department of Energy's announcement in January that it would spend as much as $625 million to fund two to five quantum research centers. The move is part of the U.S. National Quantum Initiative signed into law by President Donald Trump on Dec. 21, 2018.

But what, really, is this thing called a quantum internet? How does it work? Figueroa, enraptured by his vision, told me of his plan with contagious enthusiasm, laughing sometimes as if it were all so simple that a child (or even an English major) could understand it. Not wanting to disappoint, I nodded my head and pretended that I knew what the hell he was talking about.

And, after spending two days with Figueroa last summer, following him around the campus of Brookhaven and the nearby Stony Brook, getting a firsthand look at his futuristic equipment, talking with other physicists around the world, reading a few books and perusing dozens of articles and studies, I began to kind of, sort of, get it. Not in all its unsettling depths, but in the general way that I understand how an internal-combustion engine goes vroom or why a toilet bowl flushes. And you can, too.

Untangling Entanglement

Leading me to the back room of his laboratory at Stony Brook, where he heads the quantum information technology group, Figueroa shows me a large table covered with a labyrinth of tiny mirrors, lasers and electronics. "This is where we create these photons that carry superpositions," he says, "that then we can send into the fiber. OK? It's very simple."

Curiously, all the implications of the quantum internet can be traced back to an experiment so straightforward you can do it in your living room. Called the double slit experiment, it was first performed more than 200 years ago by British polymath Thomas Young.

When shining a beam of light at a flat panel of material cut with two slits side-by-side, Young saw that the light passing through the slits created an interference pattern of dark and bright bands on a screen behind the panel. Only waves – light waves – emanating from the two slits could make such a pattern. Young concluded that Isaac Newton, who published a particle theory of light in 1704, was wrong. Light came in waves, not in particles.

Leading me to the back room of his laboratory at Stony Brook, where he heads the quantum information technology group, Figueroa shows me a large table covered with a labyrinth of tiny mirrors, lasers and

electronics. “This is where we create these photons that carry superpositions,” he says, “that then we can send into the fiber. OK? It’s very simple.”

Curiously, all the implications of the quantum internet can be traced back to an experiment so straightforward you can do it in your living room. Called the double slit experiment, it was first performed more than 200 years ago by British polymath Thomas Young.

When shining a beam of light at a flat panel of material cut with two slits side-by-side, Young saw that the light passing through the slits created an interference pattern of dark and bright bands on a screen behind the panel. Only waves – light waves – emanating from the two slits could make such a pattern. Young concluded that Isaac Newton, who published a particle theory of light in 1704, was wrong. Light came in waves, not in particles.

Think on that. A single particle of light was in two places at once. That meant tickling a particle in one place should make it giggle in the other. Observing it in one place should reveal something about its twin. Erwin Schrödinger called the phenomenon entanglement – the very thing that Figueroa and other researchers are harnessing now to send information. Simply put, adding information, such as a message or data, to a particle in one location will make the data appear at the other location: the essence of teleportation.

But how, I ask Figueroa, do all these wild ideas work in practice, with nuts and bolts and physical devices?

“Let me show you where the magic happens,” he says.

Thanks for the Quantum Memories

“It’s just equipment and optics,” he tells me, pointing to an array of lasers and mirrors configured on a large table. “This is what people call Lego for adults.” On one end, a laser aims high-energy blue photons at a crystal, which breaks each one into a pair of lower-energy red photons; each of the two resulting red photons is now entangled with the other. Figueroa points out the path the photons take from mirror to mirror. “They do boop, boop, boop, boop, boop-boop-boop-boop. This is why we have this beautiful system. This is working, actually. This is beautiful,” he says.

Once entangled, one red photon is sent a short distance to a detector in Figueroa’s lab down the hall, while the other can be sent a dozen miles away to a detector at the Brookhaven National Lab. The differing distances would cause the two photons’ arrival times to fall slightly out of sync, which would disrupt their entanglement. To prevent that, Figueroa had to find a way to coordinate the arrival times of each down to the sub-nanosecond.

But how? Other quantum labs freeze their stay-at-home photons to near-absolute zero as a way of tapping the brakes. Figueroa’s innovation, by contrast, works at room temperature: an inch-long glass tube containing a fog of trillions of rubidium atoms. That first morning when I visit Figueroa’s lab, he puts one of these tubes in my hand.

“What is it?” I ask him.

He smiles and says, “A quantum memory.”

Back when he was pursuing his doctorate at the University of Konstanz in Germany, Figueroa tells me, he had asked his professor if it would be possible to build a system that would work at room temperature without costly, complex freezers.

“I don’t think so,” he was told. “But prove me wrong.”

So, he did. By bouncing photons off a series of carefully placed mirrors and bombarding a mist of rubidium atoms with a network of lasers, Figueroa discovered that he could tune the wavelengths of entangled photons to broadcast a signal that electrons in the rubidium fog could receive. Voila! The entangled state of the photon is transferred, momentarily, into the entire cloud of atoms. A fraction of a nanosecond later, the entangled photon moves on, arriving at the detector at the same moment as its twin.

Incredibly, since completing his doctorate in 2012, igueroa has miniaturized the entire system for holding quantum memories into a portable device smaller than a carry-on suitcase, small enough to mount on an ordinary rack of computer servers at a data center – a crucial innovation if a quantum internet is ever to go mainstream. As his colleague and collaborator Dimitrios Katramatos tells me later that day: "They are portable, right? So, we loaded some of them up in a van one day and brought them from Stony Brook to Brookhaven."

"He drove his wife's van," Figueroa says with a laugh. "Ever since we have called it the Quantum Van."

Entanglement Swapping

Another problem remains, however – one that neither Figueroa nor Katramatos (nor any other quantum engineer in the world) has fully figured out so far: how to successfully transmit quantum-entangled photons via fiber-optic cables past a barrier that appears around the 60-mile mark. Beyond it, photons unintentionally interact with the cable, its housing or even sunlight from above-ground, thereby destroying its entanglement.

The proposed solution, Figueroa explains, is something called "entanglement swapping." And quantum engineers around the world are competing to apply the concept to a working prototype.

"The idea has by now been around for 20 years," says Mikhail Lukin, a leading quantum theoretician and experimentalist at Harvard University. "Up to now, no one has succeeded in building one capable of being used in a practical application. As far as I understand, that's what [Figueroa]'s group is trying to do."

To explain his plan, Figueroa leads me into a small meeting room, where he has it all mapped out on a whiteboard.

"Let me show you something really cool," he says.

Instead of creating only one pair of entangled photons and trying to send it to a lab 100 miles away, he explains, a second set of entangled pairs are created in two different substations located at the 25-mile and 75-mile marks. These substations will shoot one photon of the pair toward each other and the other toward the closest of the two labs. When one photon from each of the two pairs meets at the 50-mile mark, they will become entangled, automatically entangling the other remaining photons in the distant laboratories. Once this entanglement has been shared, the information Figueroa wanted to send can be teleported to the lab 100 miles away, overcoming the barrier.

The Quantum Future

And what about teleporting not just information, not just messages, but also particles, molecules, cells or Captain Kirk? When the first experimental demonstration of entanglement was reported in December 1997, IBM physicist Charles H. Bennett told The New York Times: "It would be utterly infeasible to do it even on something as small as a bacterium." (Bennett, it should be pointed out, had coined the term quantum teleportation four years earlier, so you would think he would be correct.)

But 21 years later, in the fall of 2018, Oxford University researchers reported exactly what Bennett had said was “utterly infeasible”: the entanglement of a living bacterium with a photon of light. Not all physicists were persuaded by the findings, however, based as they were on the Oxford team’s analysis of another group’s experiment. But then, nobody knows how far the quantum revolution will go – certainly not Figueroa.

“Many of the things these devices will do, we are still trying to figure it out,” he tells me. “At the moment, we are just trying to create technology that works. The really far reaches of what is possible are still to be discovered.”

Before leaving him, I ask Figueroa how his friends, family and neighbors try to understand his cryptic work. He tells me a story about his father-in-law. Back when Figueroa was conducting postdoctoral research in Germany, his wife’s father came to visit. After giving him a two-hour tour of the lab, Figueroa asked him what he thought of it all.

“I didn’t understand a word you said in there,” his father-in-law said, “but I know it’s the most amazing thing I have ever seen.”

I could empathize. That’s how I felt before visiting Figueroa, interrogating him repeatedly over the phone, and reading his papers with far-out titles like “A Single-Atom Quantum Memory” and “Quantum Memory for Squeezed Light.” But after all that, the whole thing began to make sense to me. And I hope it does now for you, too.

Kind of.

3 Easy Steps to Build a DIY Quantum Internet

- **Step 1.** To build a quantum internet, you begin by entangling two photons so they behave like a single unit, no matter how far they might be separated. Easy peasy. To do this, take one high-energy blue photon, generated by a laser, and put it through a crystal that splits the photon into two lower-energy red photons. Now those photons are permanently entangled. Kind of like Brad Pitt and Angelina Jolie, entangled till the end of time as Brangelina. Now go ahead and send one of those photons to your pal, Steven Spielberg, and keep the other one for yourself.

  Which one did you send, Brad or Angelina? Until Spielberg looks through his peephole to see who’s on the other side of the door, you both have a random, 50-50 chance of seeing one or the other. In the quantum world, everything exists in a statistical blur. But that’s OK, because Brad and Angelina are just your conduit for sending information from one to the other.

- **Step 2.** To send a meaningful message from Brad to Angelina, you need a third photon. Let’s call this one Jennifer Aniston. Put Jennifer through a polarizer – like the polarized lenses used in sunglasses – to set her atomic pole to a particular position on the vertical and horizontal axes. This gives you a quantum bit, or qubit, which can be a 0 or 1 at the same time. Similar to the 0s and 1s of digital data, qubits can be strung together to encode any message you want to send – say, the script for a new movie.

- **Step 3.** You’re almost there! Now you need to entangle the qubit called Jennifer with the photon called Brad, who you’ve been hanging onto ever since you sent Angelina to Spielberg. To do that, put both Jennifer and Brad into a beam splitter. When you do, Jennifer becomes entangled not only with Brad, but also with Angelina, by virtue of the preexisting Brangelina connection. All three of them are entangled with each other.

Now get this: Because photons are so sensitive, the very act of measuring them (to be sure that they are in fact entangled) destroys them. So, both Brad and Jennifer vanish in your lab. But wait: Spielberg still has Angelina. And Angelina is still entangled with the information that Jennifer had. This means – ta da! – the information Jennifer was carrying has now been teleported, instantaneously, to Spielberg's photon.

You did it! Now you can only hope Spielberg remembers to thank you at the Oscars. – D.H.

02 Oct 2020

52 BT and Toshiba use Quantum Cryptography to create 'unhackable' network

by Steve McCaskill

https://www.techradar.com/in/news/bt-and-toshiba-use-quantum-cryptography-to-create-unhackable-network

BT and Toshiba are celebrating the UK's first industrial deployment of a quantum secure network in Bristol.

The 6 km network uses standard Openreach fibre to connect sites belonging to the National Composites Centre (NCC) and the Centre for Modelling & Simulation (CFMS) across the city.

The project was chosen because of the sensitive nature of the data sent between the two organisations. Both have interests in the aerospace, energy, and automotive industries and deemed standard networking and security technologies to be insufficiently secure. Instead, data was stored and transported on physical storage – a much more inefficient, time-consuming, and inherently insecure method than what quantum networking promises.

Instead, data was stored and transported on physical storage – a much more inefficient, time-consuming, and inherently insecure method than what quantum networking promises.

Quantum networking

Whereas classical computing architectures store information in binary (1 or 0) bits, Quantum computing uses subatomic particles' ability to exist in multiple states at the same time. This means Quantum computers can store significantly more information and compute issues much more quickly.

Quantum computing has huge implications for the financial, military and healthcare sectors among others as it can expedite research projects. And while some have concerns that this increase in computing power could render most encryption measures obsolete, it also opens the door for even more powerful security measures through quantum cryptography.

This network in Bristol is protected by Quantum Key Distribution (QKD), a supposedly 'unhackable' technique for sharing encryption keys between locations using a single stream of photons. Multiplexing compatibility allows both data and keys to be transmitted on the same fibre, essentially doubling network capacity, and allows for the distribution of 1000s keys per second.

BT and Toshiba say the new network demonstrates a tangible benefit to industry and the viability of QKD to transmit sensitive data across fibre.

“This first industrial deployment of a quantum-secure network in the UK is a significant milestone as we move towards a quantum-ready economy,” declared Professor Andrew Lord, head of optical technology at BT.

“The power of quantum computing offers unprecedented opportunity for UK industry, but this is an essential first step to ensure its power can be harnessed in the right way and without compromising security.”

“Our solution can be implemented on standard BT fibre infrastructure and is applicable to a wide range of different applications, allowing organisations to ensure the long-term security of their data and protect it from even the most powerful computers,” added Dr. Andrew Shields, head of quantum technology at Toshiba Europe.

“With the UK government’s assertion earlier this month that it wants to be the ‘world’s first quantum-ready economy’, quantum-secure networks are vital to it achieving this ambition, and we’re excited to be at the forefront of making this a reality.”

The UK government has expressed a desire to be at the forefront of the field, believing it can play a vital role in the connected economy and accelerate Industrial Internet of things (IIoT) deployments. A National Quantum Computing Centre (NQCC) is expected to open in 2022 as part of the £1 billion National Quantum Technologies Programme.

BT itself has constructed a commercial-grade test network link that spans 125km between its Adastral Park R&D facility in Suffolk and the University of Cambridge and links to the wider UK Quantum Network (UKQN) – a collaboration between industry and academia.

53 Quantum Computing is a Challenge for Cryptography

by Maurizio Di Paolo Emilio

https://www.eetimes.com/quantum-computing-is-a-challenge-for-cryptography/

Quantum computing promises significant breakthroughs in science, medicine, financial strategies, and more, but it also has the power to blow right through current cryptography systems, therefore becoming a potential risk for a whole range of technologies, from the IoT to technologies that are supposedly hack-proof, like blockchain.

Cryptography is everywhere – in messages from WhatsApp, online payments, eCommerce sites. Perhaps we cannot see it, but our data are transformed several times to avoid being tracked. “Simple” Wi-Fi is protected by the Wi-Fi Protected Access 2 (WPA2) protocol. Every credit card transaction is protected by the Advanced Encryption Standard (AES). These are different encryption methods with different mathematical problems to solve.

In order to keep ahead of potential security problems, the length of the encryption keys is gradually increasing, and the algorithms are gradually becoming more sophisticated. The general principle is that the longer the key length, the more difficult it is for a brute force to attack and break it. These are attacks in which cyber criminals make thousands of attempts to force keys until they find the right one.

All of this remains true with classic computers that operate with bits and bytes. If and when quantum computers that use qubits come into play, however, then the story changes. In the case of encryption keys, quantum computers are able to process an enormous number of potential results in parallel.

In an interview with EE Times, Jason Soroko, CTO of PKI, Sectigo, said “A traditional computer has two states: on and off, which is why we call them binary computers and often refer to ones and zeros that represent those on and off states. A quantum computer can also use a third state known as a superposition, which gives a quantum computer a unique capability."

He added, "traditional computers measure their data in bits, but quantum computers utilize a 'quantum bit' or qubit. That unique capability enables a quantum computer to perform integer factorization very quickly, which is why current cryptographic algorithms that are based on factorization are potentially vulnerable in the future. A traditional binary computer solves that mathematical problem slowly, whereas a quantum computer with an efficient algorithm can solve that problem much more quickly. That efficient algorithm known as 'Shor's Algorithm', when coupled with a quantum computer with enough stable qubits, will theoretically be able to break current cryptographic algorithms such as RSA and Elliptic Curve (ECC)."

Progress in quantum computing would jeopardize the use of PKI X.509 (RSA, ECDSA) certificates used today for authentication and digital signature algorithms: all must be protected by new quantum-resistant algorithms to remain secure.

Quantum computing and security

Quantum computers are based on the idea of encoding the digital encoding value into a property of an elementary particle, called "quantum bit" or qubit. According to quantum mechanics, the operations in these quantum CPUs are performed by transforming the state of the elementary particles.

Above, Soroko referred to an algorithm that will probably be the thing that make quantum-era hacking so destabilizing. Named after its developer, Peter Shor, the algorithm allows the factorization of a whole number in polynomials; the second part speeds up the search for a value or a function inversion.

Asymmetric encryption provides a pair of public-private keys with an extremely complex mathematical relationship. The secret private key supports creating a digital signature that can be verified using the public key, protected by a mathematical principle called "unidirectional function."

Shor's algorithm solves the mathematical problem underlying many asymmetric encryption algorithms, or public-private key, such as the RSA algorithm.

The advent of quantum processors capable of performing the Shor's algorithm would make asymmetric algorithms such as RSA, ECC, or all cryptographic algorithms based on integer factoring mathematical problems, discrete logarithms, and discrete logarithms on elliptical curves completely insecure.

Quantum cybersecurity

What is stopping quantum computers overcoming normal ones is that they are difficult to build and maintain stability. Any slight change in temperature or vibration can cause calculations to fail and force you to start again from scratch. That said, many companies, including Google and IBM, have made a lot of progress.

Before the quantum computing becomes common, everyone is advised to secure their data, because when a quantum computer falls into the hands of a cyber-criminal, it will take little time to decipher just about anyone's data in an astonishingly brief amount of time.

The RSA and ECC algorithms are practically impossible to decipher with brute force methods on a traditional computer. But they're not impossible to a quantum computer with sufficient stable qubits. Quantum computers can therefore threaten all communications, trade, and finance.

Companies and IT managers are working on protection quantum-based cybersecurity attacks. Learning and training are important factors to consider. We already have quantum-safe encryption algorithms, but they are not yet widely used. There are many reasons for this. First of all, these new algorithms are not yet standardized. It is an essential step so that everyone can refer to the same algorithm. The second reason is that it is necessary to inventory with extreme precision, where what and why encryption is used for existing platforms and services.

“Quantum-resistant cryptographic algorithms have been proposed and are currently undergoing a selection process by NIST, an authority dealing with certifications and standards. Quantum resistance comes from choosing a mathematical approach that is difficult for both traditional and quantum computers. Current cryptographic algorithms such as RSA and ECC are based on algebraic problems, whereas quantum-resistant algorithms are based on solving entirely different problems. As an example, lattice-based cryptography uses a geometric, rather than algebraic approach, rendering a quantum computer’s special properties less effective. In other words, good cryptography requires a tough problem to solve, and lattice-based cryptography is tough for both classical and quantum computers to solve, making it a good candidate to be the basis of an approach for a post-quantum cryptographic algorithm,” said Soroko.

It is important to gain practical experience with the new post-quantum algorithms and to test the emission and use of safe quantum certificates. As the cryptographic community standardizes on quantum-safe algorithms, Soroko pointed out Sectigo has announced the release of ‘Sectigo Quantum Labs’ which combines a web resource meant to provide education on this subject, as well as a toolkit that enables the user to experiment with quantum-resistant algorithms and issue hybrid certificates. The solution includes the basic tools needed to create quantum-safe certificates for a variety of use cases, along with sample applications showing the use of quantum-safe algorithms.

New quantum secure schemes have been proposed in the literature. Most of them have a public key and signature size significantly larger than those used today. Although post-quantum signatures may work well for some use cases, there are concerns about their size and processing costs on technologies using X.509 certificates.

The X.509 standard defines as a digital certificate, an electronic document associated with a natural person or a computer service that certifies their identity; it consists of a public and a private key provided by the Certification Authority that awaits its validity. In general, being a certificate of identity, it is used in authentication systems based on public key infrastructure (PKI); moreover, it can be used to sign and encrypt e-mail messages.

“Quantum-safe certificates are x.509 based PKI certificates where the keypair is generated with a quantum-resistant algorithm. In the future, we will likely be living in a world where both traditional and post-quantum algorithms will be used at the same time because it will be difficult to rip and replace all of the PKI infrastructures in existence. Hybrid certificates will have both traditional and quantum-safe keys and signatures, which will help to bridge the gap between systems that have been designed to take advantage of the new algorithms, and those that cannot,” said Soroko.

Almost all the algorithms in use with public-private key and used daily for web browsing are subject to Shor’s algorithm that makes them insecure. There is, therefore, the need to develop new algorithms in a so-called post-quantum phase, i.e. identify and create cryptographic algorithms that will remain secure after the advent of quantum processors. The researchers are proposing several post-quantum cryptographic algorithms with different approaches and based on different mathematical problems that would imply a high consumption of network resources.

54 IonQ Unveils New 32-Qubit Quantum Computer

by Matt Swayne

https://thequantumdaily.com/2020/10/02/ionq-unveils-new-32-qubit-quantum-computer/

IonQ unveiled its next generation quantum computer system, according to a news release. The new hardware features 32 perfect qubits with low gate errors, giving it an expected quantum volume greater than 4,000,000.

According to the release, the new system consists of perfect atomic clock qubits and random access all-to-all gate operations for efficient software compilation of applications. It will be first available via private beta, and then commercially available on Amazon Braket, where IonQ's 11 qubit system is generally available for customers today, and Microsoft's Azure Quantum. Pre-existing IonQ customers and partners, including 1QBit, Cambridge Quantum Computing, QC Ware, Zapata Computing and more are excited to experience the benefits of the new system, enabling them to drive towards the first wave of quantum applications.

The company's trapped-ion quantum computers have a proven track record of outperforming all other available quantum hardware. With this new iteration, IonQ continues to lead the quantum computing field into the future. IonQ is already working on its next two generations of quantum computers, with each new system expected to be both exponentially more powerful and smaller in size than the last.

"In a single generation of hardware, we went from 11 to 32 qubits, and more importantly, improved the fidelity required to use all 32 qubits," said IonQ CEO & President Peter Chapman. "Depending on the application, customers will need somewhere between 80 and 150 very high fidelity qubits and logic gates to see quantum advantage. Our goal is to double or more the number of qubits each year. With two new generations of hardware already in the works, companies not working with quantum now are at risk of falling behind."

The team said it's based on many years of research.

"The technology underpinning IonQ's new system is based on decades of proven research and advancements, and our unique architecture provides essential computational efficiencies as the system scales up," said IonQ Co-Founder & CTO Jungsang Kim. "This cornerstone moment provides the foundation for IonQ to rapidly grow and continue to perfect our systems."

IonQ Co-Founder & Chief Scientist Chris Monroe said that the latest version is pushing the boundaries of what a quantum computer can do.

"Demonstrating the first successful quantum logic gate in 1995 was almost an accident, but doing so opened a path forward towards deploying quantum computers on previously unsolvable problems," said Monroe. "The new system we're deploying today is able to do things no other quantum computer has been able to achieve, and even more importantly, we know how to continue making these systems much more powerful moving forward." One way is to fix errors through circuit encoding, capitalizing on a recent demonstration of quantum error correction in a nearly identical system. Monroe says "with our new IonQ system, we expect to be able to encode multiple qubits to tolerate errors, the holy grail for scaling quantum computers in the long haul." This encoding requires just 13 qubits to make a near-perfect logical qubit, while in other hardware architectures it's estimated to take more than 100,000."

Algorithms have already been tested on the machine, according to IonQ partners.

“We design quantum machine learning algorithms to drive performance on near-term hardware,” said Iordanis Kerenidis, Head of Algorithms International, QC Ware. “We collaborated with IonQ in implementing QC Ware’s quantum classification algorithm on their system, and the excellent results attest to their unique approach and demonstrated performance.”

Denise Ruffner, Chief Business Officer, Cambridge Quantum Computing, said, “IonQ and Cambridge Quantum Computing are working together to create and implement applications for quantum computers, for the benefit of CQC’s customers, and are excited to see what new applications are possible with IonQ’s newest generation.”

The achievement is also getting notice from several funders. IonQ has raised $84 million in funding, recently announcing new investment from Lockheed Martin, Robert Bosch Venture Capital GmbH (RBVC) and Cambium. Previous investors include Samsung Electronics, Mubadala Capital, GV, Amazon, and NEA.

“IonQ represents one of the most promising approaches to quantum computing that is both scalable and does not require any significant materials science or manufacturing breakthroughs,” said Francis Ho, Senior Vice President and Managing Director, Samsung Catalyst Fund. “The company’s unique combination of academic research and experience plus proven performance has led to their system demonstrating industry leading performance and helping break new ground in quantum computing.”

Alaa Halawa, Head of US Ventures, Mubadala Capital, added, “We believe IonQ is the most promising and advanced technology for developing quantum computers at scale. This latest milestone represents decades of academic research and experience, proven performance, and superior technology. This latest breakthrough is also particularly exciting for industrial companies in areas of material science and petrochemicals, enabling new applications that are crucial for enhancing competitiveness in the market.”

The company’s two co-founders were recently named to the National Quantum Initiative Advisory Committee (NQIAC).

55 Leading Cybersecurity Provider of Patented, Cryptographic-Based Technologies Quantum-Resistant Encryption Protocol, To Make Data Breaches Obsolete

by James Dargan

https://thequantumdaily.com/2020/10/02/leading-cybersecurity-provider-of-patented-cryptographic-based-technologies-quantum-resistant-encryption-protocol-to-make-data-breac

TQD has already highlighted in features the threat quantum information science could pose in cybersecurity issues in the future. To compound the fact, we have also put a spotlight on some of the main players and budding startups within the space, too.

Companies like QuintessenceLabs and Crypta Labs, along with others, are playing their part to secure us from malign attacks using the sorcery of qubits. And as the threat becomes greater, more players – realizing there will be money to be made – will come into existence.

One startup that has already noticed this and whose founding team is loaded with decades of experience in the cybersecurity and cryptography industries is BLAKFX.

Fight quantum with quantum

– Vikram Sharma, CEO QuintessenceLabs

BLAKFX

BLAKFX's two founders, CEO and president Robert Statica and COO Kara Coppa, established the startup in 2017. With offices in New York City, New Jersey and Los Angeles, BLAKEFX models itself as 'the leading B2B and B2G cybersecurity provider of patented, cryptographic-based technologies with a quantum-resistant encryption protocol'.

The crown jewel in the startup's products and cybersecurity services is the Helix22™ SDK, the world's first user-to-user encryption solution. The magic of this product is it secures clients' data when not being used, during transportation and in use. Furthermore, BLAKFX's Helix22™ SDK offers five layers of encryption:

- AES1
- TwoFish
- AES2
- ThreeFish
- Snow3G

All this has been made possible by the work of Statica and Coppa, BLAKFX's brains. As already mentioned, the pair have years in cybersecurity and cryptography, and can, by experience alone, brag king size of why their QC cyber solutions are as good as anyone else's on the market.

With over seventy patents to his name, inventor Statica is also a scientist, technologist, engineer, and professor. With a Ph.D. in business administration from Northcentral University in San Diego, he began his career as an aircraft engineer in the late 1980s. In line with this, Statica has worked at NASA as an aerospace engineer and the Planetary Society, where he was a space mission scientist advisor. In 2012, he cofounded Wickr, a private collaboration platform.

Coppa is BLAKFX's other founder. With two decades of experience in cybersecurity, she has worked in the intelligence, military and financial services industries, too, bringing her wealth of knowledge to those fields. Coppa has an MS in information systems from the New Jersey Institute of Technology, and before founding Wickr (along with Statica) she worked in information security as an engineer and manager.

> In math we trust
>
> – BLAKFX

What I've covered here is only the tip of the iceberg in regards to BLAKFX's offerings and potential. Products in ransomware auditing as a service (RaaS) and technical surveillance countermeasures – along with others – could make BLAKFX one of the go-to companies on the market in the coming months and years.

01 Oct 2020

56 Achieving Quantum Volume 128 on the Honeywell Quantum Computer

by Honeywell

https://www.honeywell.com/en-us/newsroom/news/2020/09/achieving-quantum-volume-128-on-the-honeywell-quantum-computer

We achieved a Quantum Volume of 128 on our Quantum Computer in late September 2020.

This and future increases in the capabilities of quantum computers will empower our customers to achieve results beyond what they thought was possible.

“Honeywell has made a commitment to shape and accelerate the development of Quantum Computing and bring its power to our customers,” said Tony Uttley, President of Honeywell Quantum Solutions.

“Our differentiated technology, exemplified by the high-fidelity and fully-connected qubits with mid-circuit measurement and qubit reuse, enables our customers to push the frontier of quantum computing applications. And what is really exciting is that this is still just the beginning.”

“Our differentiated technology, exemplified by the high-fidelity and fully-connected qubits with mid-circuit measurement and qubit reuse, enables our customers to push the frontier of quantum computing applications. And what is really exciting is that this is still just the beginning.”

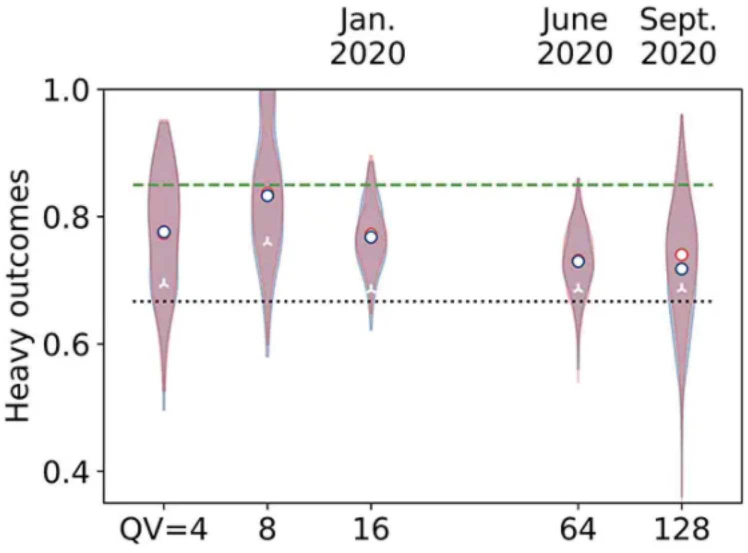


Figure 1: The plot above shows the heavy outcomes for Honeywell Quantum Solutions’ tests of quantum volume and the dates when each test passed. All tests are above the 2/3 threshold to pass the respective Quantum Volume. Circles indicate heavy outcome averages and the violin plots show the histogram distributions. Data colored in blue shows system performance results and red shows modeled, noise-included simulation data. White markers are the lower 2-sigma error bounds.

The system successfully passed the Quantum Volume 128 test outputting heavy outcomes 71.78% of the time, which is above 2/3 threshold with 99.934% confidence. The average single-qubit fidelity is 99.97(1)% and the average two-qubit gate fidelity is 99.54(7)% with fully-connected qubits.

Our systems are accessible directly through Honeywell or through Microsoft Azure Quantum. In addition to offering high-fidelity, fully-connected qubits, our system features a unique mid-circuit measurement capability, which enables users to explore new classes of algorithms and to greatly reduce the number of qubits needed for certain algorithms.

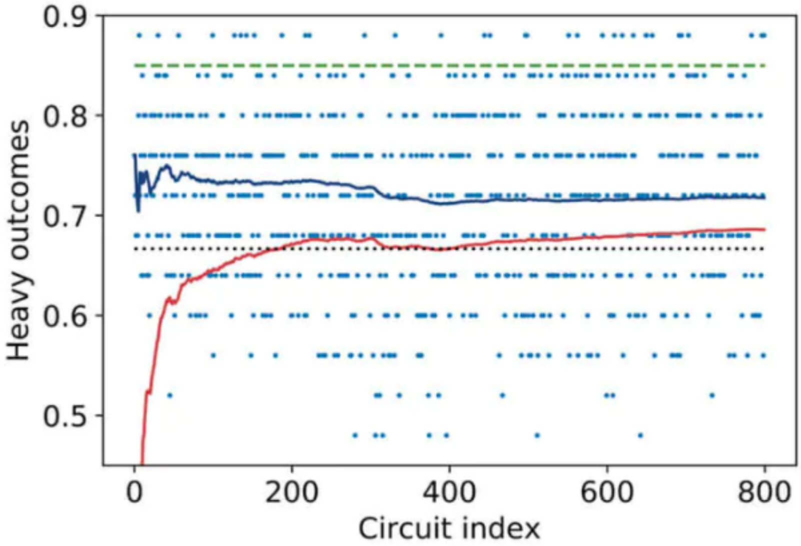


Figure 2: The plot above shows the individual heavy outcomes for each Quantum Volume 128 run. The blue line is an average of heavy outcomes and the red line is the lower 2-sigma error bar which crosses the 2/3 threshold after 186 circuits.

57 Now IMO is hit by cyber-attack, as CMA CGM says it suspects a data breach

by Gavin van Marle

https://theloadstar.com/now-imo-is-hit-by-cyber-attack-as-cma-cgm-says-it-suspects-a-data-breach/

CMA CGM yesterday revealed it may have suffered a data breach during the recent cyber-attack.

As the French carrier works on restoring its systems, it said: "We suspect a data breach, and are doing everything possible to assess its potential volume and nature."

However, it added that its IT technicians had made progress in restoring its systems.

"Today, the back-offices (shared services centres) are gradually being reconnected to the network, thus improving bookings and documentation processing times," it said.

And it reminded customers that online bookings could still be made through the INTTRA portal, as well by spreadsheet via email, and said EDI messages were also secure.

It told them: "Maritime and port activities are fully operational. We are providing alternative and temporary processes for your bookings and are committed to processing them as quickly as possible."

Meanwhile, cyber criminals have continued their assault on the maritime sector after the industry's governing body, the International Maritime Organization (IMO), admitted it had also suffered a cyber-attack when its website went down yesterday.

"The interruption of service was caused by a cyber-attack against our IT systems," it said today. "IMO is working with UN IT and security experts to restore systems as soon as possible, identify the source of the attack and further enhance security systems to prevent recurrence."