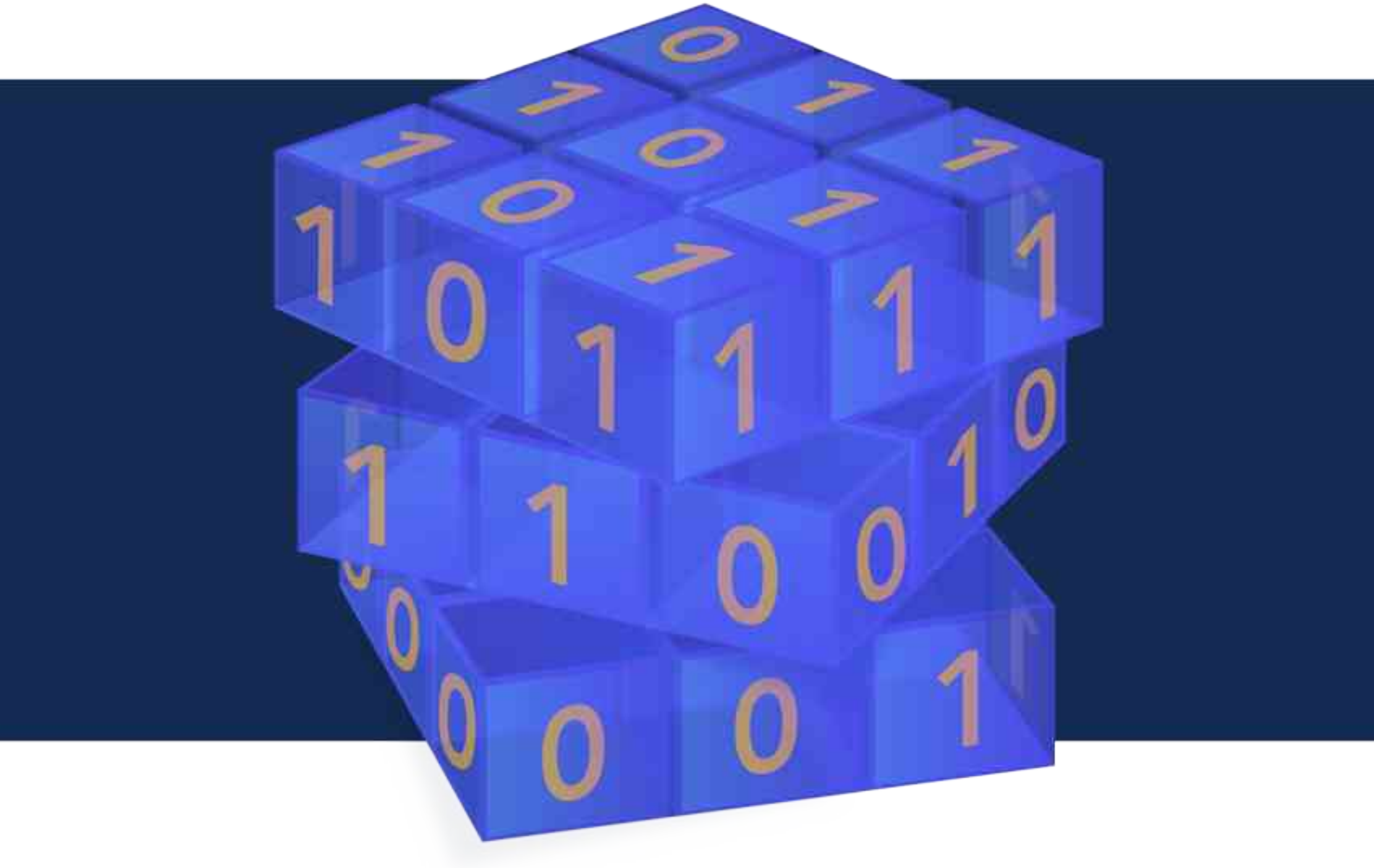
Crypto News

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

December 01, 2021



Contents

Editorial

SEATTLE, WA – December, 1st, 2021. This edition of Crypto News will be the last of 2021 so don't let it pass you by! Let's start with a look at article #2. The governments of certain countries have a strong interest in accessing encrypted messages processed by the tech industry while also holding the tech industry to stringent cyber security requirements. Predictably, this is causing confusion for the tech industry and concerns for their customers. So who's correct here? The governments, the tech industry, or is there perhaps a middle ground we're not discussing yet? After that, scroll down to article #24. This article is particularly of interest to those readers who are currently invested in cryptocurrency. The backbone of cryptocurrency is blockchain technology which is secured by public key cryptography. The current trajectory of quantum computers have a high probability of "cracking" public key cryptography which has the potential to threaten the cryptocurrency world. All hope is not lost though! Cryptocurrency companies have started to move towards or develop quantum proof cryptography algorithms. Read the article to learn more about what cryptocurrency companies can do to help protect themselves and their customers in a post-quantum world. Perhaps none of this sounds interesting to you. Fear not! There's plenty more in the newsletter and not enough space here to do it all justice so be sure to scroll through. We'll
see you all again in the new year!

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

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

1.Quantum physicist David Deutsch bags Isaac Newton medal and Prize

by Michael Banks

https://physicsworld.com/a/quantum-physicist-david-deutsch-bags-isaac-newton-medal-and-prize/

The quantum physicist David Deutsch has won the 2021 Isaac Newton Medal and Prize for "founding the discipline named quantum computation and establishing quantum computation's fundamental idea, now known as the 'qubit' or quantum bit". Presented by the Institute of Physics (IOP), which publishes Physics World, the international award is given annually for "world-leading contributions to physics".

Deutsch's honour formed part of the IOP's wider 2021 awards, which recognize everyone from early-career scientists and teachers to technicians and subject specialists. This year saw various changes to the IOP's awards process, including self-nominations allowed for the first time and greater publicity to encourage a wider pool of applicants. Of those winners who chose to include data about their personal background, some 19% stem from a Black, Asian or minority ethnic group.

Born in Haifa, Israel, Deutsch studied physics at the University of Cambridge before doing a PhD at the University of Oxford. After several years at the University of Texas at Austin, he returned to Oxford, where he is currently based. Deutsch is also a founding member of the university's Centre for Quantum Computation, which opened in 1998.

Deutsch has been awarded the Newton medal and prize thanks to his research in quantum theory. In 1985 Deutsch published his ground-breaking work that detailed the relationship between quantum theory and the universal quantum computer. Four years later he then developed the theory of quantum computational gates and networks, which is today the basis of quantum-information science.

In the early 1990s Deutsch proved that a quantum computer would be able to solve problems that require exponentially more computational time on a classical computer due to its restricted modes of computation. His work opened the possibility that the properties of quantum mechanics could have tangible and useful applications in computing. Indeed, today there are several commercial quantum computers being developed by companies and governments worldwide.

The Isaac Newton Medal and Prize attracts an award of £1000 and is the only one of the IOP's prizes that is open to physicists worldwide. Previous winners include Thomas Kibble, Deborah Jin and Ed Witten."I am honoured and also very happy that the Institute of Physics recognizes the significance of quantum computation as a fundamental part of physics," Deutsch told Physics World.

2.Government must prove its plans to police encryption work, says ex-cyber security chief

by Bill Goodwin

https://www-computerweekly-com.cdn.ampproject.org/c/s/www.computerweekly.com/news/252510066/Government-must-proves-its-plans-to-police-encryption-work-says-ex-cyber-security-chief?amp=1

The government has been challenged to set out how it can "clearly and transparently" allow law enforcement agencies and intelligence services access to encrypted communications while still maintaining communications security.

Ciaran Martin, founder and former CEO of GCHQ's National Cyber Security Centre, and now a professor at the University of Oxford, said the onus should be on the government to set out detailed technical options for scrutiny and debate on its plans to monitor encrypted communications.

His comments came amid increasingly polarised arguments between the Home Office, which argues that end-to-end encryption allows people to spread child abuse images or terrorist content, and cryptographers who warn that weakening encryption would undermine the security of everyone.

Home secretary Priti Patel has singled out Facebook, calling for it to abandon plans to extend end-to-end encryption from its WhatsApp service to Messenger and Instagram, on the grounds that encryption would assist criminals.

But Martin said in a lecture organised by the Bingham Centre for the Rule of Law, that the use of end-to-end encryption must be permitted unless a technical compromise can be found that is acceptable to the tech industry and cryptography experts.

"If a suitable technical compromise solution that commands widespread expert and industry confidence cannot be reached, then security must win, and end-to-end encryption must continue to expand, legally unfettered for the betterment of our digital homeland," he said.

Onus is on government

The government argues that the tech industry should enable government access to encrypted messages, while at the same time demanding the highest levels of cyber security.

“Surely though, the onus is on the government, not the industry, to set out clearly and transparently how they believe these two seemingly irreconcilable objectives can be met in the same regulatory package?” said Martin.

Technology companies and cryptographers claim that the government’s demands are simply not possible - the government is in effect, trying to argue against the laws of mathematics.

If the UK and US governments can read encrypted messages, so potentially can criminals, or hostile nation states such as North Korea or Russia.

Extensively researched proposals to find a compromise, including proposals by Ian Levy, technical director of the National Cyber Security Centre to use “virtual crocodile clips” to listen in to encrypted communications, have failed to convince sceptics, said Martin.

Plans by Apple to introduce “client-side scanning” technology to detect child abuse images before they are encrypted provoked a backlash from the world’s top cryptographic experts and internet pioneers and have now been suspended.

An expert report identified over 15 ways in which states or malicious actors, and targeted abusers, could turn the technology around to cause harm to others or society.

Martin spoke sceptically about the Home Office programme, known as the Safety Tech Challenge, which is offering a prize to companies that can implement end-to-end encryption “without opening the door to greater levels of child sexual abuse”.

If anyone can develop the innovative technology the Home Office envisages, he or she is likely to be worth a lot more than the £85,000 promised by Her Majesty’s Treasury.

“The government has some way to go to convince people that it has not just launched a competition to develop the digital age equivalent of alchemy,” he said, in a speech first reported in Prospect magazine.

He said much of the public intervention at ministerial level over the last three years appears to have been spent “shouting at Facebook,” which has been slower than other tech companies to implement end-to-end encryption across its platforms.

The prospect of Facebook fully encrypting its services has alarmed organisations such as the National Society for the Prevention of Cruelty to Children (NSPCC), which reported in 2019 that half of the reports of online abuse came from Facebook platforms. In the US the figure is closer to 90%.

Home secretary Patel, along with other interior ministers of the Five Eyes countries, wrote an open letter to Facebook CEO Mark Zuckerberg the same year, urging him not to introduce end-to-end encryption.

But Martin said it was unreasonable to conclude that Facebook accounts for the vast majority of online child sexual abuse. The figures simply reflected the fact that Facebook has not yet implemented end-to-end encryption.

“The difficult reality is that these policy interventions are, in effect, demanding that one very large and increasingly unpopular company does not do what most of its competitors have already done,” he said.

“Of all the legitimate complaints we can have about Facebook’s business practices, catching up with the rest of the industry on what has become broadly-accepted best practice in messaging platform security is surely not top of the list.”

Government powers

The Investigatory Powers Act 2016 gives the government powers to issue Technical Capability Notices (TCNs) to require communications companies to remove encryption or provide communications in intelligible form, when required.

Martin said the government needs to be transparent and honest with the public over its approach to encryption.

“If it is to be the case that end-to-end encryption poses such a threat to public safety that its implementation and use must be constrained by law, then the government needs to be absolutely open about what that means,” he said.

That means the government should level with the public that digital protections will not be as good as they might be otherwise, but the greater good demands that law enforcement can access encryption.

There should also be more openness about what sort of Technical Capability Notices are needed, why and how they are applied.

“If we learned anything from Snowden, it’s that the state needs to seek informed consent for what they do in this space. Relying on a general sense of ‘those with nothing to hide have nothing to fear’ is a terrible idea’,” he said.

Encryption cannot be wished away

Martin said the revolution in digital security brought about by encrypted services such as Signal cannot be wished away, “Canute like”.

“It is hard to see a blanket ban on end-to-end encrypted services, and it is hard to see an increasingly security- and privacy-savvy population doing anything other than flock to them, the bad minority as well as the good majority,” he said.

The difficulties for law enforcement are real, he said. adding he had no doubt that if Facebook moves to end-to-end encryption it would make the job of law enforcement harder.

But he said the widespread use of encryption is the latest cycle in a game of cat and mouse between technology and law enforcement.

Technology changes, criminals use the new technology, the good guys catch up, the technology changes, and the cycle starts over again.

“Looked at this way, end-to-end encryption is just another practical operational issue, not an issue of principle,” he said.

Even in the aftermath of the NSA whistleblower Edward Snowden, governments did not "go dark", they "went spotty". They had access to a lot of data but not all the data they needed or had access to before.

Often, though not always, there are other ways for law enforcement to get hold of the information they need.

For example, in 2015 the FBI attempted to compel Apple to unlock the iPhone of the San Bernardino terrorist, but after a protracted legal battle the FBI managed to access the phone in a different way.

"Would it really have been better," Martin asked, "if the US government had won and compelled Apple to do something that would potentially compromise all of its phones?"

He suggested that both sides in the argument over end-to-end encryption should approach the problem with "fairness" and "generosity of spirit". "Instead of traducing the good intentions and vital work of policing and intelligence with offensive accusations that they're 'playing the child abuse card,' why not redouble efforts to help bring offenders to heel in the new technological dispensation?"

3.A Nanoantenna for Long-Distance, Ultra-Secure Quantum Communication

by OSAKA UNIVERSITY

https://scitechdaily.com/a-nanoantenna-for-long-distance-ultra-secure-quantum-communication/

Information storage and transfer in the manner of simple ones and zeros—as in today's classical computer technologies—is insufficient for quantum technologies under development. Now, researchers from Japan have fabricated a nanoantenna that will help bring quantum information networks closer to practical use.

In a study recently published in Applied Physics Express, researchers from Osaka University and collaborating partners have substantially enhanced photon-to-electron conversion through a metal nanostructure, which is an important step forward in the development of advanced technologies for sharing and processing data.
Classical computer information is based on simple on/off readouts. It's straightforward to use a technology known as a repeater to amplify and retransmit this information over long distances. Quantum information is based on comparatively more complex and secure readouts, such as photon polarization and electron spin. Semiconductor nanoboxes known as quantum dots are materials that researchers have proposed for storing and transferring quantum information. However, quantum repeater technologies have some limitations—for example, current ways to convert photon-based information to electron-based information are highly inefficient. Overcoming this information conversion and transfer challenge is what the researchers at Osaka University aimed to address.

"The efficiency of converting single photons into single electrons in gallium arsenide quantum dots—common materials in quantum communication research—is currently too low," explains lead author Rio Fukai. "Accordingly, we designed a nanoantenna—consisting of ultra-small concentric rings of gold—to focus light onto a single quantum dot, resulting in a voltage readout from our device."

The researchers enhanced photon absorption by a factor of up to 9, compared with not using the nanoantenna. After illuminating a single quantum dot, most of the photogenerated electrons weren't trapped there, and instead accumulated in impurities or other locations in the device. Nevertheless, these excess electrons gave a minimal voltage readout that was readily distinguished from that generated by the quantum dot electrons, and thus didn't disrupt the device's intended readout.

"Theoretical simulations indicate that we can improve the photon absorption by up to a factor of 25," says senior author Akira Oiwa. "Improving the alignment of the light source and more precisely fabricating the nanoantenna are ongoing research directions in our group."

These results have important applications. Researchers now have a means of using well-established nano-photonics to advance the prospects of upcoming quantum communication and information networks. By using abstract physics properties such as entanglement and superposition, quantum technology could provide unprecedented information security and data processing in the coming decades.

4.New Platform for Quantum Computing?

by Aalto University

https://scitechdaily.com/new-platform-for-quantum-computing-artificial-material-mimics-quantum-entangled-rare-earth-compounds/

Physicists have created a new ultra-thin two-layer material with quantum properties that normally require rare earth compounds. This material, which is relatively easy to make and does not contain rare earth metals, could provide a new platform for quantum computing and advance research into unconventional superconductivity and quantum criticality.

The researchers showed that by starting from seemingly common materials, a radically new quantum state of matter can appear. The discovery emerged from their efforts to create a quantum spin liquid which they could use to investigate emergent quantum phenomena such as gauge theory. This involves fabricating a single layer of atomically thin tantalum disulfide, but the process also creates islands that consist of two layers.

When the team examined these islands, they found that interactions between the two layers induced a phenomenon known as the Kondo effect, leading to a macroscopically entangled state of matter producing a heavy-fermion system.

The Kondo effect is an interaction between magnetic impurities and electrons that causes a material's electrical resistance to change with temperature. This results in the electrons behaving as though they have more mass, leading these compounds to be called heavy fermion materials. This phenomenon is a hallmark of materials containing rare earth elements.

Heavy fermion materials are important in several domains of cutting-edge physics, including research into quantum materials. "Studying complex quantum materials is hindered by the properties of naturally occurring compounds. Our goal is to produce artificial designer materials that can be readily tuned and controlled externally to expand the range of exotic phenomena that can be realized in the lab," says Professor Peter Liljeroth.

For example, heavy fermion materials could act as topological superconductors, which could be useful for building qubits that are more robust to noise and perturbation from the environment, reducing error rates in quantum computers. "Creating this in real life would benefit enormously from having a heavy fermion material system that can be readily incorporated into electrical devices and tuned externally," explains Viliam Vaňo, a doctoral student in Liljeroth's group and the paper's lead author.

Although both layers in the new material are tantalum sulfide, there are subtle but important differences in their properties. One layer behaves like a metal, conducting electrons, while the other layer has a structural change that causes electrons to be localized into a regular lattice. The combination of the two results in the appearance of heavy fermion physics, which neither layer exhibits alone.

This new heavy fermion material also offers a powerful tool for probing quantum criticality. “The material can reach a quantum-critical point when it begins to move from one collective quantum state to another, for example, from a regular magnet towards an entangled heavy fermion material,” explains Professor Jose Lado. “Between these states, the entire system is critical, reacting strongly to the slightest change, and providing an ideal platform to engineer even more exotic quantum matter.”

“In the future, we will explore how the system reacts to the rotation of each sheet relative to the other and try to modify the coupling between the layers to tune the material towards quantum critical behavior,” says Liljeroth.

5.Zurich Instruments launches its first Qubit Controller offering a full qubit control system in a single instrument

by Julien Levallois
https://www.swissquantumhub.com/zurich-instruments-launches-the-first-qubit-controller-offering-a-full-qubit-control-system-in-a-single-instrument/

The Zurich Instruments SHFQC Qubit Controller offers a full room-temperature qubit control system for up to 6 superconducting qubits in a single instrument. The SHFQC provides channels for driving high-fidelity single- or two-qubit gates, perform single-shot multiplexed qubit readout, and perform fast feedback or error correction protocols. Like other elements of the Zurich Instruments Quantum Computing Control System (QCCS), all channels of the SHFQC work at microwave frequencies with great spectral purity and stability, so that users do not need to rely on tedious mixer calibration. Operation of the SHFQC through Zurich Instruments’ Python APIs, LabOne, and the LabOne QCCS Software gives access to an intuitive approach to demanding tasks such as automated system tune-up or the execution of complex algorithms, thus enabling system up-time and measurement speed-up.

Concept

The SHFQC provides a full qubit control setup for controlling, reading out and performing fast feedback on up to 6 superconducting qubits as a single instrument. The setup is fully software-operated and thus simple to reconfigure. When using several SHFQCs, the control system can be extended to support larger qubit numbers and thus adds fast local feedback to global error correction.

Thanks to the operating range from DC to 8.5 GHz and the combination with a linear amplification chain, each of the 6 high-performance control channels of the SHFQC can drive any single- or two-qubit gate in a short time and at the relevant qubit frequency. The readout channel of the SHFQC includes signal generation and detection, and a state-of-the-art signal processing chain that can discriminate between the states of several qubits, qutrits or ququads with high fidelity and in real time. The measurement results are swiftly distributed to all control channels for fast feedback and local error correction protocols. Additional signal processing functions, such as a real-time oscilloscope, fast resonator spectroscopy and powerful sequencers in all channels, round up the capabilities of the SHFQC.

Together, the instrument's features enable fast bring-up of the quantum device as well as a reduced system downtime and a significant speed-up of measurements.

As the maturity of available superconducting quantum processors increases, the number of different qubit control techniques can be expected to decrease. This may determine a shift away from individually designed control setups and towards carefully engineered commercial solutions. Until today, small systems with a handful of qubits did not benefit from application-specific, high-performance and versatile solutions that are quick to set up and intuitive to operate. "The SHFQC extends the reach of our next-generation QCCS to smaller setups. Now researchers with a few qubits can profit from integrated, mixer-calibration-free frequency conversion and even more application-specific, high-performance functionality," says Dr. Tobias Thiele, Application Scientist for Quantum Technologies at Zurich Instruments. "Nonetheless, the possibility to scale to larger system sizes remains," Dr. Thiele adds, "as multiple SHFQCs can be combined with other elements of the QCCS to support larger setups."

Software support and system integration

The reduced latency and increased flexibility afforded by processing qubit information within a single instrument can be key to the success of local feedback operations such as fast active or ancilla reset. As part of the QCCS, the SHFQC can also be integrated into new or existing setups consisting of up to 18 other instruments such as the HDAWG Arbitrary Waveform Generator, the SHFSG Signal Generator and the PQSC Programmable Quantum System Controller to scale from few qubits to 100 qubits and beyond. The LabOne software, the new LabOne QCCS Software and the LabOne Python APIs help users handle any combination of QCCS instruments as one system that remains well-synchronized and controlled by a single software interface. Tasks such as experiment tune-up, automated calibration and the execution of complex algorithms therefore become simple and intuitive.

6.Cryptolab aims to secure firm position in global homomorphic encryption market

by Lim Chang-won
https://www.ajudaily.com/view/20211123110024142

As a pioneer in homomorphic encryption research, Cheon Jung-hee, a prominent mathematician and cryptographer in South Korea, has pushed for the early introduction of quantum-resistant cryptography technology, saying that if quantum computers are commercialized, existing encryption algorithms, which were difficult to solve even after decades, will be resolved within minutes.

Binary digital electronic computers are based on transistors and capacitors with data encoded into binary digits (bits). Quantum computation uses quantum bits or qubits. Theoretically, a quantum computer would gain enormous processing power and perform tasks using all possible permutations simultaneously.

Quantum cryptography is an essential security solution for safeguarding critical information. Data encoded in a quantum state is virtually unhackable without quantum keys which are basically random number tables used to decipher encrypted information. Even though current, publicly known, experimental quantum computers lack the processing power to break any real cryptographic algorithm, many cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat.

Cheon, a Seoul National University professor of mathematical sciences, established Cryptolab, a data security start-up, in 2017 to commercialize his homomorphic encryption technology called "HEaaN" that provides the ability to analyze data while being encrypted. It is advertised as the only solution that provides real-number calculation among homomorphic encryptions that can perform calculations while protecting sensitive information.

Cryptolab holds patents on the original technology of homomorphic encryption for the arithmetic of approximate numbers. With HEaaN, Cheon aims to have a firm position in the international application market. "Whether it is a single or cooperative model, we are preparing to enter the global homomorphic encryption application market," he said in an interview with Aju Business Daily.

The main target is the United States, the professor said, adding that his company is trying to develop a technology on fast homomorphic encryption. Big tech companies such as IBM and Microsoft are implementing their own homomorphic encryption. However, Cheon said with a firm conviction that his technology is far better and verified through performance evaluation results.

"The potential of homomorphic encryption that protects personal information and makes it possible to utilize is endless, but it is still perceived as unfamiliar to people," Cheon said. Yet, prospects are bright as homomorphic encryption companies are attracting a lot of investment in the overseas venture investment market, he said, citing Cornami, an American high-performance computing company that develops break-through computing architecture for real-time environments.

"Since algorithms themselves are rarely accelerated, the goal is to supply our library to such companies," the professor said. "Compared to existing ciphers that were used only for data protection, homomorphic encryption is suitable for an active role in protecting while using data. In the future, this technology will become more important, and South Korea will be able to lead the field of homomorphic cryptography."

Homomorphic encryption schemes have difficulty in commercialization because the size of ciphertexts exponentially increases when iterating operations with it. HEaaN discards small values of numbers to increase the calculation speed and minimizes inefficiencies that occur during computation with homomorphic encryption. "HEaaN's problem is that there is a limit to processing speed due to a lot of computing resources, and we are developing hardware accelerators to solve it," Cheon said.

In partnership with a medical data venture, Cryptolab is involved in a project to apply homomorphic encryption to the standardization and management of medical data in hospitals. The startup has also attracted investment from Samsung Electronics and LG Uplus (LGU+). Samsung's investment is related to homomorphic encryption, while Cheon works with LGU+ to commercialize post-quantum cryptography (PQC) that refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer.

PQC does not require separate network infrastructure to distribute cryptographic keys because it can be applied flexibility to different sections of wired and wireless networks that require encryption. PQC technology is useful in hospitals and other areas that handle sensitive information. Cheon said HEaaN and PQC are based on the same technology. "It's a technology that comes from one root," he said, describing HEaaN as a younger brother of PQC.

7.QuTech Introduces a Quantum Network Explorer

https://quantumcomputingreport.com/qutech-introduces-a-quantum-network-explorer/

QuTech, a Dutch organization that is a collaboration between the TU Delft and TNO, has introduced a web site where users can simulate various aspects of a quantum internet. At this time, the simulations are performed on a classical computer but it is conceivable that this web site might allow allow users to try experience on real quantum communications hardware sometime in the future. The web site provides graphical animations of various quantum communications operations. There are currently three pre-configured applications available for beginners which include a Distributed CNOT, State Teleportation (also known as Quantum Teleportation), and Quantum Key Distribution (QKD). The website also includes an Application Development Kit for Quantum Network Explorer (QNE-ADK) for researchers who want to build their own experiments. To learn more about the Quantum Network Explorer, you can visit their web site to try out the sample applications, read the documentation, or get instructions on how to install the QNE-ADK software.

8.Qunnect Announces Sale of First Commercial Quantum Memory

by Matt Swayne

https://thequantuminsider.com/2021/11/22/qunnect-announces-sale-of-first-commercial-quantum-memory/

Qunnect, Inc., a Quantum Networking company, announces the sale of the world's first commercial Quantum Memory to Brookhaven National Laboratory. Quantum Memories are critical components for enabling future quantum-secure networks, as they support distributed entanglement communication protocols, and serve as core components in quantum repeaters.

Qunnect's Quantum Memory stores and releases single photons, on-demand, while preserving their quantum state at a fidelity above 95%. Unlike other quantum memory technologies, Qunnect is unique in providing a solution that does not require extreme cooling or vacuum support infrastructure for operation, a key design consideration for real-world deployment and scaling. All devices are also housed in standard server-rack form-factor for installation in existing fiber hubs.

The Quantum Memory is the core of Qunnect's Quantum Repeater product suite which includes a device to generate entangled photons, ultra-high precision timing and frequency network references, fiber channel calibrators, and a transaction station to perform entanglement distribution protocols. Qunnect is engineering these devices to interface with low interface loss and telecommunications infrastructure.

"We are very proud to be the first company to bring a quantum memory to the commercial market. As fiber-based quantum testbeds are being built across the globe, we look forward to supporting their infrastructure." said Qunnect CEO, Noel Goddard. "We are also grateful to our investors and the Federal agencies who enabled this accomplishment, and continue to support our vision of realizing prototypes of the full Quantum Repeater product suite in early 2022."

9.2021 ACM Gordon Bell Prize Awarded to Chinese Team for Closing Google's 'Quantum Supremacy Gap'

by Matt Swayne
https://thequantuminsider.com/2021/11/22/2021-acm-gordon-bell-prize-awarded-to-chinese-team-for-closing-googles-quantum-supremacy-gap/

CM, the Association for Computing Machinery, named a 14-member team, drawn from Chinese institutions, recipients of the 2021 ACM Gordon Bell Prize for their project, Closing the "Quantum Supremacy" Gap: Achieving Real-Time Simulation of a Random Quantum Circuit Using a New Sunway Supercomputer.
The members of the winning team are: Yong (Alexander) Liu, Xin (Lucy) Liu, Fang (Nancy) Li, Yuling Yang, Jiawei Song, Pengpeng Zhao, Zhen Wang, Dajia Peng, and Huarong Chen of Zhejiang Lab, Hangzhou and the National Supercomputing Center in Wuxi; Haohuan Fu and Dexun Chen of Tsinghua University, Beijing, and the National Supercomputing Center in Wuxi; Wenzhao Wu of the National Supercomputing Center in Wuxi; and Heliang Huang and Chu Guo of the Shanghai Research Center for Quantum Sciences.

Quantum supremacy is a term used to denote the point at which a quantum device can solve a problem that no classical computer can solve in a reasonable amount of time. Teams at Google and the University of Science and Technology of China in Hefei both claim to have developed devices that have achieved quantum supremacy.

According to the Gordon Bell Prize recipients, determining whether a device has achieved quantum supremacy for a given task (in a specific scenario) begins with sampling the interactions of the different quantum bits (qubits) in a random quantum circuit (RQC). As the number of possible interactions among qubits in a random quantum circuit is staggeringly large, simulating their interactions is a problem well-suited for a high-performance computer. However, the quantum physics behind the entangled qubits requires that the classical binary bits used in a supercomputer store and compute the information with exponentially-increasing complexity.

In their Gordon Bell Prize-winning work, the Chinese researchers introduced a systematic design process that covers the algorithm, parallelization, and architecture required for the simulation. Using a new Sunway Supercomputer, the Chinese team effectively simulated a 10x10x (1+40+1) random quantum circuit (a new milestone for classical simulation of RQC). Their simulation achieved a performance of 1.2 Eflops (one quintillion floating-point operations per second) single-precision, or 4.4 Eflops mixed-precision, using over 41.9 million Sunway cores (processors).

The project far outpaced state-of-the-art approaches to simulating an RQC. For example, the most recent effort, using the Summit supercomputer to simulate a random quantum circuit of the Google Sycamore quantum processor (which has 53 qubits), was estimated to take 10,000 years to perform. By contrast, the Chinese team's approach employing the Sunway supercomputer takes only 304 seconds for a simulation of similar quantum complexity.

The Chinese team explained that they undertook this challenge because achieving real-time simulation of an RQC using a supercomputer would aid both in the development of quantum devices and in bringing algorithmic and architectural innovations within the traditional supercomputing community.

The ACM Gordon Bell Prize tracks the progress of parallel computing and rewards innovation in applying high performance computing to challenges in science, engineering, and large-scale data analytics. The award was presented today by former ACM President Cherri M. Pancake and Professor Mark Parsons, Chair of the 2021 Gordon Bell

Prize Award Committee, during the International Conference for High Performance Computing, Networking, Storage and Analysis (SC21), which was held in St. Louis, Missouri, and virtually for those who could not attend.

10.UK government publishes guidance on security rules for tech takeovers

by Lindsay Clark

https://www.theregister.com/2021/11/17/uk_government_publishes_guidance_national/

The UK government has published guidance describing what technologies may be caught within the National Security and Investment Act 2021, which is set to give ministers the power to halt mergers and acquisitions.

The legislation, due to come into force in January, gives the government leeway to scrutinise buyouts and investments, impose certain conditions on an acquisition or, if necessary, unwind or block it. The statement issued this week, did, however say it expects to do this rarely, while the "vast majority" ofdeals will be able to proceed without delay.

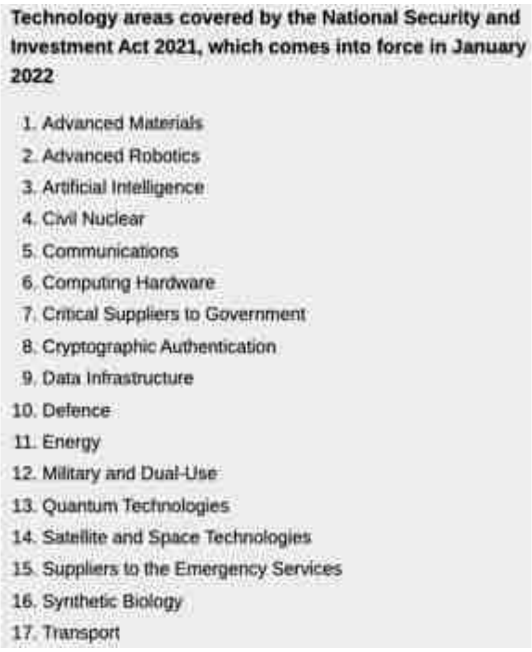
The issue of technologies considered important to national security has become relevant to the tech sector in recent months, as stories about chip plant ownership and advanced materials hit the news. In the new guidance, the government said it wanted businesses and investorsto get ready for the changesin the law. It wants them to assess whether the government must be notified of an acquisition and understand what they are to expect when they gothrough the notification and assessment process.

Business minister Lord Callanan said the government would not hesitate to intervene where necessary to protect our national security.

"The new investment screening process willbesimpler and quicker,givinginvestors andfirmsthecertaintythey need to do business,and I urge them to make sure they are ready for the changesbefore they comeinto forcein January," he said.

The guidance says that "if an entity you are acquiring performs a certain activity, it could put you in scope of the National Security and Investment Act and you may be legally required to tell the government about it (known as a 'mandatory notification'). This guidance tells you what these activities are."

The guidance covers a long list of technologies, not all of them relevant to IT, but included in the box below.



Technology areas covered by the National Security and Investment Act 2021, which comes into force in January 2022

1. Advanced Materials
2. Advanced Robotics
3. Artificial Intelligence
4. Civil Nuclear
5. Communications
6. Computing Hardware
7. Critical Suppliers to Government
8. Cryptographic Authentication
9. Data Infrastructure
10. Defence
11. Energy
12. Military and Dual-Use
13. Quantum Technologies
14. Satellite and Space Technologies
15. Suppliers to the Emergency Services
16. Synthetic Biology
17. Transport

The list includes Artificial Intelligence. Regarding AI, it says investors should consider if their target does research into, develops or produces goods, software or technology that uses AI and whether that technology is used to identify or track advanced robotics or "cyber security."

To determine if a qualifying entity you are seeking to acquire is in-scope of the "Computing Hardware" part of the regulations calls for an assessment of whether the target company owns, creates, supplies or exploits the intellectual property of hardware products or functions.

The rules stretch to data infrastructure, which includes data centre operators, cloud storage service providers, managed service providers, specialist or technical service providers, software providers with access to customer data. They do not cover off-the-shelf software though.

Within scope for cryptographic authentication are technologies that identify a physical person using an access token, or use a biometric property of an individual to access a restricted area.

The guidance also includes chip-and-pin technology and e-passports in this category.

The government is putting forward two pieces of secondary legislation. The Procedure for Service Statutory Instrument sets out how the government sends and receives documents under the Act while the Form and Content of Notification Forms Statutory Instrument sets out what information is required in the Act's notification forms, which parties can submit to the government under the Act.

In a statement on National Security and Investment Act 2021 the government made it clear it would not set out the circumstances in which national security is, or may be, considered at risk, reflecting a policy to ensure that national security powers are sufficiently flexible to protect the nation.

In September, the UK government issued a surprise public interest intervention notice against the proposed takeover of Welsh advanced materials specialist Perpetuus Group, claiming it represents a potential threat to national security.

Founded in 2013, the Perpetuus Group's main subsidiary is Perpetuus Advanced Materials, a company that recently boasted of a breakthrough in the production of plasma-processed P-doped graphene and the creation of a "drop reactor" prototype which could produce surface-modified graphene in one-thirtieth the time of its previous approach.

In July, Prime Minister Boris Johnson promised a national security investigation into a China-backed corporation's takeover of Britain's largest producer of semiconductors, Newport Wafer Fab (NWF) in a deal reported to be worth £63m ($87m).

Yesterday, the Competition and Markets Authority said it was moving its probe of the Nvidia/ Arm merger into Phase 2, and will undertake deeper scrutiny. Digital Secretary Nadine Dorries stated explicitly this is due to "national security" issues.

11.Quantum Computing Takes Off: A Look at the Evolution of Quantum Technology and Patents

by Nick Brestoff

https://www.ipwatchdog.com/2021/11/20/quantum-computing-takes-off-a-look-at-the-evolution-of-quantum-technology-and-patents/id=140271/

Towards the end of 2019, I was finishing a book, AI Concepts for Business Applications. The last chapter was titled, “The Future.” I wrote about quantum computing and a version of deep learning that was related: a “quantum walk neural network.”

In 1980, the idea of a quantum processing unit was proposed. Such a processing unit doesn’t use the 1s and 0s with which we’re familiar. That “classical” way of thinking is the way we think, with a 1 for true and a 0 for false, and combinations—for example, a “false positive.” Quantum computing is based on a “superposition” of states called “quantum bits” or “qubits” for short. But there’s a big difference between the way we think and the way nature behaves.

In 1981, the late Caltech professor, Richard Feynman (a Nobel Prize co-winner for his work with “quantum electrodynamics”) summed it up: “Nature isn’t classical, dammit, and if you want to make a simulation of nature, you’d better make it quantum mechanical, and by golly it’s a wonderful problem, because it doesn’t look so easy.”

Now, quantum computing is beginning to emerge. It started with hardware:

- In March of 2017, IBM announced an open Application Programming Interface (API) called IBM Q, where Q means quantum.

- In December of 2017, not to be outdone, Microsoft announced a preview version of a developer kit with a programming language called Q#.

- In January of 2018, the world of neural networks, which includes a convolutional neural network (CNN), primarily for images, and a recurrent neural network (RNN), primarily for text, expanded to include a Quantum Walk Neural Network (QWNN). The QWNN paper is entitled “Quantum Walk Inspired Neural Networks for Graph-Structured Data” was written by Stefan Dernbach (then a PhD student at the University of Massachusetts College of Information and Computer Sciences); Arman Mohseni-Kabir (then a graduate student in physics at UMass Amherst); Don Towsley (Dernbach's PhD advisor); and Siddarth Pal (a scientist with BBN Raytheon Technologies).

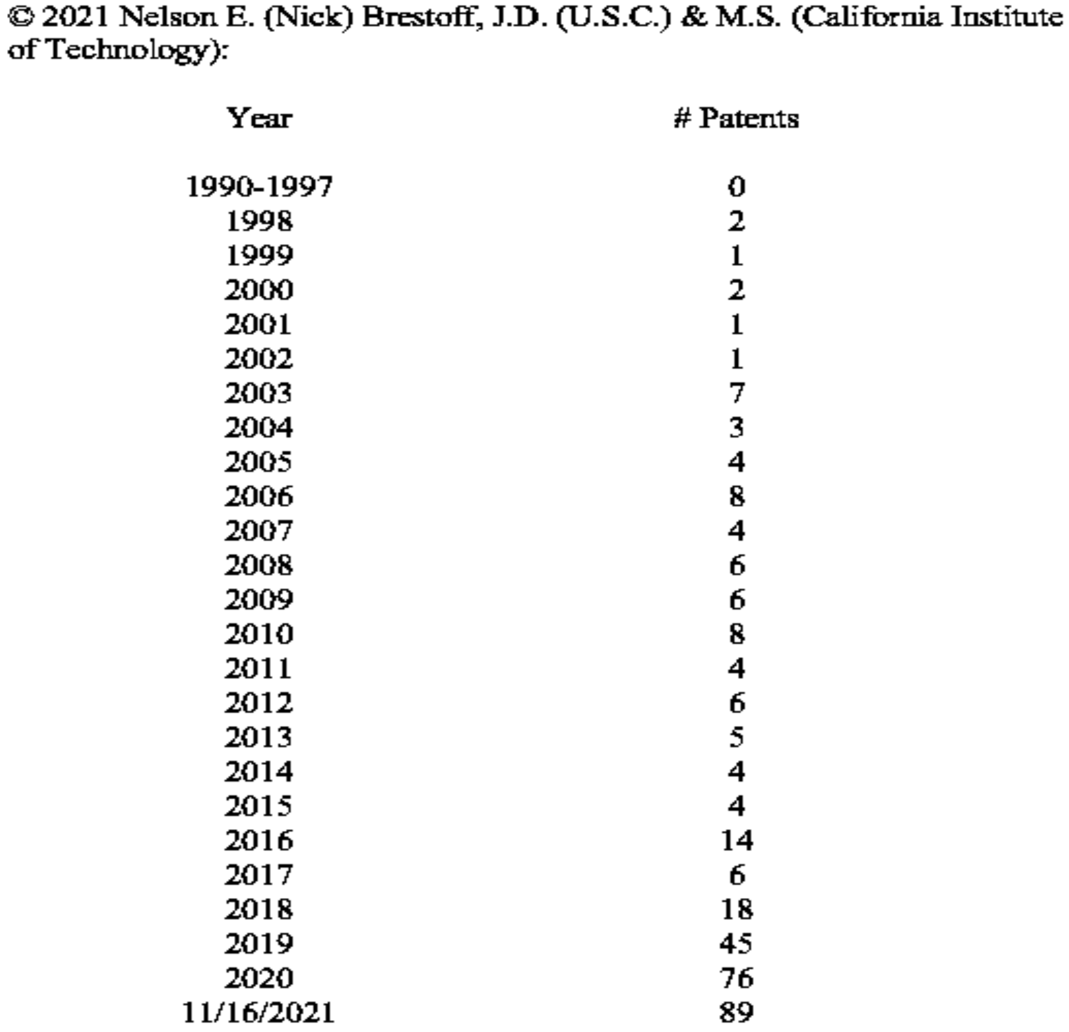
In their Abstract, they wrote, "A QWNN learns a quantum walk on a graph to construct a diffusion operator which can be applied to a signal on a graph. We demonstrate the use of the network for prediction tasks for graph structured signals."

Note the phrase "prediction tasks." That's what deep learning known for being able to do, that is, once trained with labeled data, a model "for the label" (or category or classification) is able to identify images or text from a blizzard of input the model's never seen before, and yet find the needles that match to the model. Such models have become known as "prediction machines."

- In March of 2018, Google's Quantum AI Lab announced a 72-qubit processor called Bristlecone.
- On July 19, 2018, Google announced an open-source framework called Cirq (where the C is short for cryogenic) and plans for a Bristlecone cloud.
- On January 8, 2019, IBM announced IBM Q System One as the first integrated quantum system for commercial use.
- On February 21, 2019, Google announced a cryogenic controller that used only two milliwatts of power.
- In May 2019, Microsoft announced that, in the summer of 2019, it would open-source parts of its Quantum Developer Kit on GitHub, including the Q# compiler and quantum simulators.
- On October 23, 2019, in a Nature paper, Google announced "quantum supremacy." The paper was entitled, "Quantum supremacy using a programmable superconducting processor." As Google summarized the advance in the Abstract:

> A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2,3,4,5,6,7] to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years."

From this much, you may gather that the field of quantum computing had finally made it to the launch pad of an "emerging technology."



© 2021 Nelson E. (Nick) Brestoff, J.D. (U.S.C.) & M.S. (California Institute of Technology):

Year	# Patents
1990-1997	0
1998	2
1999	1
2000	2
2001	1
2002	1
2003	7
2004	3
2005	4
2006	8
2007	4
2008	6
2009	6
2010	8
2011	4
2012	6
2013	5
2014	4
2015	4
2016	14
2017	6
2018	18
2019	45
2020	76
11/16/2021	89

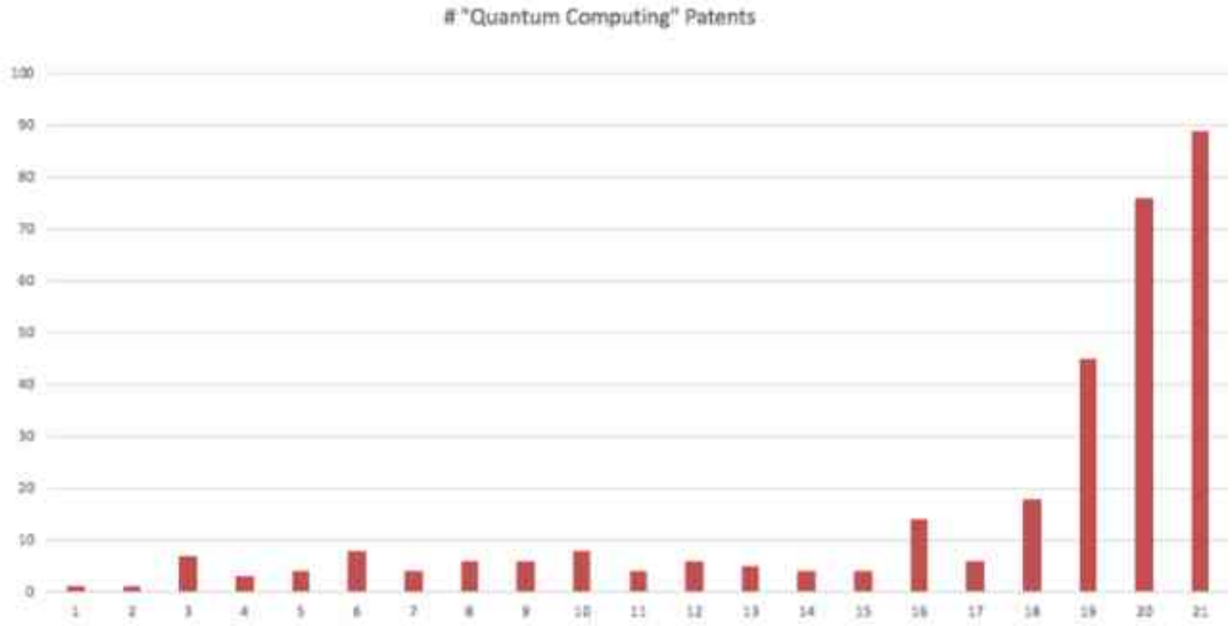
Quantum Computing Patents

With that history, let's switch to patents. I've previously presented bar graphs for two emerging technologies: deep learning and blockchain. These graphs are based entirely on searching the U.S. Patent and Trademark Office's (USPTO's) patent database.

As before, I searched for a key word or phrase in the Claims field of the USPTO database. For the annual data, I searched the USPTO for "quantum computing" in the Claims and for the Issue Date on an annual basis. The bar graph for "quantum computing" is surprisingly similar to the bar graphs for deep learning and blockchain.

THE QUANTUM COMPUTING PATENT LAND RUSH

The total on November 16, 2021 was 322. Keep in mind that the 2021 total is for a partial year as of November 16. Since there are six more Tuesdays in 2021 (when new patents are announced), I'll predict a year-end for 2021 of 150 or more.



If you compare this bar graph to the graphs for deep learning and blockchain, the conclusion is readily apparent. We are living in a time when deep learning, blockchain and quantum computing are rapidly emerging, and almost simultaneously. Wonders we cannot now foresee will come from these advances.

12.Universal photonic quantum processor sets new size record

by Soroush Khademi
https://physicsworld.com/a/universal-photonic-quantum-processor-sets-new-size-record/

Scientists from QuiX Quantum and the adaptive quantum optics group at the University of Twente in the Netherlands have built the largest universal photonic quantum processor to date. The processor works by applying adjustable phase shifts to the optical signals going through its 12 modes and then merging the signals in adjustable proportions. The precision of its fabrication allows single photons to interfere as they propagate, making the processor capable of quantum operations – albeit not yet at a level that could outperform classical machines.

The new device takes in 12 input optical signals, processes them and outputs the result optically, all at the standard telecommunication wavelength. The device's photonic configuration – that is, the phase shifts and the proportions of each signal being merged – determines the nature of the processing task, and users can reconfigure this by connecting it to an ordinary personal computer. In this way, the device can be programmed to perform any processing task realizable by a specific set of optical merging and phase shifting steps.

The photonic processor and its delicate engineering

To implement these steps, the device uses a series of optical components known as tuneable phase shifters and tuneable beam mergers. The latter consists of two beam mergers that combine pairs of input beams in equal proportions, plus a tuneable phase shifter. The key to making the system reconfigurable is thus to have full control over the phase shifters within the processor's photonic circuit, where each of the phase shifters is a heater that induces a very well-tuned and specific change in the effective path length of the passing optical signals via a phenomenon known as the thermo-optic effect.

By satisfying a list of technical demands for the 12 modes, from high-quality microfabrication of the photonic waveguides (optical paths) to providing fast mechanisms for stabilizing the temperature of the photonic circuit, the team set a record for the number of on-chip modes with a programmable configuration that can process quantum optical inputs (such as single-photon ones). In other words, the probability of losing a single photon inside the processor is low, and furthermore, identical single photons injected to different inputs of the processor do not appear different at the output. These results have been published in *Materials for Quantum Technology*.

Characterizing the processor

To quantify the processor's reconfigurability, the team changed the processor's configuration and tested it using laser light (providing classical inputs) and photodetectors. By comparing the configuration obtained in this test with the desired one, they found the "amplitude fidelity" – a measure of similarity between different configurations – was about 93%, stretching to 98% for some target configurations.

The researchers also evaluated the processor's optical loss with the same input–output setup. They found that this was as low as 17% on average, although a significant amount of additional loss occurs at the input and output connectors. Finally, they characterized the processor's ability to preserve the identical nature of single photons. The team did this by injecting two identical, single photons simultaneously and observing a phenomenon known as Hong–Ou–Mandel interference at the single-photon detectors connected to the outputs. They found that the on-chip interference has the same visibility as the off-chip interference of the two injected single photons – meaning that single photons at the chip's output are as identical as they were at the input.

Next steps

Although this processor could, in principle, form the core of an efficient universal optical quantum computer, fabricating the other equipment needed for such a computer would be far more technically demanding. Nevertheless, there is one known computational problem for which a processor of this nature can outperform classical computers (a situation known as "quantum supremacy" or "quantum primacy") without fancier equipment. This problem is known as boson sampling and it involves predicting the output of the processor itself in a special scenario.

To understand how boson sampling works, consider what happens if we inject some identical single photons into the processor. The photons propagate through the processor and appear at the outputs where they are detected by single-photon detectors. But which detectors will find a photon? This question is inherently impossible to answer. Even if the input and the configuration is exactly the same, different detectors will be activated at the output each time we run the experiment. Nonetheless, if we run the experiment many times, we can prepare statistical samples implying the probability of different detection events. The interesting point here, from a computational point of view, is that for a big enough number of modes, classical computers cannot efficiently prepare these statistical samples (or calculate the probability distribution function for the detection events).

In 2020, researchers led by Jian-Wei Pan and Chao-Yang Lu of the University of Science and Technology of China (USTC) demonstrated quantum advantage for a similar problem using their own photonic device. The USTC team's device differs from the processor described in this study in one critical respect, however. "The authors of the 2020 paper use a static device for their proof-of-principle experiment," explains Jelmer Renema, a physicist at QuiX Quantum and the University of Twente. "We build on that result and realize full reconfigurability."

Renema goes on to explain that while the system he and his colleagues developed can run boson sampling experiments, "quantum supremacy doesn't arise with 12 modes". Nevertheless, he and other members of the research group, which is led by Pepijn Pinkse, are developing the processor. "We are working on improving the specifications of the system like reducing the optical loss and, furthermore, on increasing the number of modes. We expect to unveil a processor with 50 modes in 2022," Renema tells Physics World.

13.Physicists achieve fault-tolerant control of an error-corrected qubit

by Maria Violaris
https://physicsworld.com/a/physicists-achieve-fault-tolerant-control-of-an-error-corrected-qubit/

The quantum nature of qubits is a double-edged sword. While it could help quantum computers solve problems that are intractable on classical machines, it is also easily destroyed by noise arising from unintended interactions between qubits and their environment. To resolve this dilemma and create scalable, useful quantum computers, physicists are developing methods of correcting the errors that arise from this noise. Now, for the first time, researchers at the University of Maryland in the US have put one of these methods into practice by demonstrating fault-tolerant control of a single logical qubit – a key step towards fully error-corrected quantum computers.

To understand how this type of error correction works, think of the last time you corrected a typo. In doing so, you performed error correction on classical information. Because the meaning of a word is encoded in lots of letters, it doesn't matter much if there is a mistake in one letter – you can still identify the intended word. Quantum error correction enables us to spot and correct typos in quantum information in much the same way, by encoding the state of one logical qubit (the quantum word) within many physical qubits (the quantum letters). By performing specialized actions known as stabilizer measurements on these physical qubits, the system can then extract information about any errors that have occurred – crucially, without destroying the quantum information required for the computation. Based on this extracted information, the system can then apply the correct operations, or gates, to the physical qubits so that the overall state of the logical qubit is corrected, like replacing a letter to correct a word.

Error correction alone is not enough to enable scalable quantum computers, however. Spell-check would be counterproductive if it jumbled up other letters in the process of correcting one. Another essential condition for reliable quantum computers is that preparing the logical state, applying logic gates, detecting errors and correcting them must not introduce more errors into the system. In other words, these processes all need to be fault-tolerant, designed so that one error will not spread to cause more errors. This requirement is central to the task of building quantum computers that can solve useful problems.

Reduced error rates

In the latest work, which is published in *Nature*, researchers led by Laird Egan demonstrated the fault-tolerant control of a single logical qubit – including all the stages of preparation, logic gates and error correction. The qubits in this experiment consisted of ytterbium ions suspended above a radio-frequency Paul trap and controlled with individual laser beams. This is the hardware favoured by the quantum computing start-up IonQ, where Egan and some of his collaborators now work. The advantages of using trapped ions instead of the superconducting qubits favoured by many quantum computing firms include lower error rates and better connectivity between qubits, though there are challenges with scaling the technology.

To demonstrate fault-tolerant control, the team used a 13-qubit encoding known as the Bacon–Shor code, with nine physical qubits to encode the logical state and four qubits for error correction. These 13 qubits were arranged in a single chain, with two extra qubits on either side to ensure uniform spacing. With this system, the researchers showed that they could control the states of the logical qubits in a fault-tolerant way and correct any single-qubit errors that occurred. The team also showed that the error rates in the logical qubit were lower than the corresponding error rates when using a non-fault-tolerant protocol.

Steps towards full fault-tolerance

Egan calls the team's achievement "a really critical building block, and one that shows that we are close to achieving the error threshold where logical qubits can outperform physical qubits". He adds: "Nobody believes that you will be able to achieve this threshold without fault-tolerant error-correction protocols, and up until this work, no one had yet demonstrated fault-tolerant control of a logical qubit."

To pass that error threshold, the team's next goal is to maintain an error-free quantum state over time performing error correction repeatedly. To do this will require mid-circuit error detection, where the ions in the chain are physically moved apart so that some can be measured without affecting the others. "The hard part is when we put the chain back together, we need to make sure that ions did not heat up during their transport", explains Egan, "and if they did, we need a way to cool them back down without destroying the quantum information". The team has made progress towards this goal by showing in other work that cooling such ions is possible.

The researchers also hope to demonstrate fault-tolerant control between two qubits. To do this, they aim to implement a series of quantum operations known as a logical controlled-NOT gate, which flips the state of the second qubit conditional on the state of the first and is central to many other gates and algorithms. Egan is confident that the vision of fully fault-tolerant quantum control that outperforms physical qubits can be realized in ion traps in the near future. "Ion systems only need modest improvements to their gate fidelity, combined with mid-circuit detection, to really make this work in the next couple of years," he says.

14.Cryptographers are not happy with how you're using the word 'crypto'

by Matthew Cantor
https://www.theguardian.com/technology/2021/nov/18/crypto-cryptocurrency-cryptographers

The stadium that is home to the Los Angeles Lakers is getting a new name: the Crypto.com Arena. The name reflects the arena's new sponsorship agreement with a Singapore-based cryptocurrency trading platform. That may be good news for cryptocurrency fanatics – but perhaps not so much for another faction within the digital landscape: cryptographers.

Look up the word "crypto" in Webster's dictionary, and you'll see it refers to cryptography, which in turn is defined as "the computerized encoding and decoding of information". Search "crypto" on Google, however, and you'll see a host of top results pointing to cryptocurrencies like bitcoin and ethereum.

This lexical shift has weighed heavily on cryptographers, who, over the past few years, have repeated the rallying cry "Crypto means cryptography" on social media. T-shirts and hoodies trumpet the phrase and variations on it; there's a website dedicated solely to clarifying the issue.

'"Crypto' for decades has been used as shorthand and as a prefix for things related to cryptography," said Amie Stepanovich, executive director of Silicon Flatirons Center at the University of Colorado Law School and creator of the pro-cryptography T-shirts, which have become a hit at conferences. "In fact, in the term cryptocurrency, the prefix crypto refers back to cryptography."

It's often a losing battle, and that appears to have played out in the case of crypto.com itself.

Beginning in 1993, as the Verge reported, the crypto.com domain was owned by Matt Blaze, a cryptography expert who repeatedly rejected would-be buyers – even as the rise of cryptocurrency meant he could have made millions of dollars.

"I think calling cryptocurrencies 'crypto' is a poor choice, with bad consequences for both cryptography and cryptocurrencies," he tweeted in 2018. Ultimately, however, the domain was sold, and now if you go to Crypto.com you'll see a giant video of Matt Damon indicating that investing in cryptocurrencies is roughly as courageous as scaling an icy cliff or blasting into space.

Yet there remains an internecine feud among the tech savvy about the word.

As Parker Higgins of the Freedom of the Press Foundation, who has spent years involved in cryptography activism, pointed out, the cryptography crowd is by nature deeply invested in precision – after all, designing and cracking codes is an endeavor in which, if you get things "a little wrong, it can blow the whole thing up".

There are global debates over both cryptography – for instance, questions over whether chat services should offer "backdoors" that skirt encryption – and the regulation of cryptocurrency. "There is a need to distinguish between those two areas to avoid absolutely foreseeable confusion," Stepanovich said, a particular issue when it comes to "legislators and regulators who are not always subject matter experts in these areas, even if they are charged with overseeing them".

Higgins agreed. "Crypto as shorthand for cryptography really was in widespread use. You could talk about crypto even on Capitol Hill and people would know what you were talking about – that really did hold a lot of, forgive this, but currency."

And at a time when many still aren't sure what cryptocurrency is, the confusion over the terms just makes things muddier. "Strong cryptography is a cornerstone of the way that people talk about privacy and security, and it has been under attack for decades" by governments, law enforcement, and "all sorts of bad actors", Higgins said. For its defenders, confusion over terminology creates yet another challenge.

Stepanovich acknowledged the challenge of opposing the trend, but said the weight of history is on her side. "The study of crypto has been around for ever," she said. "The most famous code is known as the Caesar cipher, referring to Julius Caesar. This is not new." Cryptocurrency, on the other hand, is a relatively recent development, and she is not ready to concede to "a concept that may or may not survive government regulation".

She remains invested in the linguistic debate because it's so closely linked to policy. "Allowing people to develop and use encryption is hugely important in protecting human rights, privacy and protecting the basis on which cryptocurrency has been built," Stepanovich said.

“We all have hills we are willing to die on – this might be mine.”

15.IBM's New Quantum Computer Is Double the Size of China's Jiuzhang 2

by Chris Young
https://interestingengineering.com/ibms-new-quantum-computer-is-double-the-size-of-chinas-jiuzhang-2

Computing giant IBM announced that it has built the world's largest superconducting quantum computer, called Eagle, a press statement reveals. The new machine is larger than Google's Sycamore as well as China's Jiuzhang 2.

In October, researchers at China's University of Science and Technology (USTC) in Hefei announced that their quantum computer Jiuzhang 2 worked using 60 superconducting qubits, and that it was a staggering 10 million times faster than Google's Sycamore quantum computer.

Now, IBM's new Eagle processor will more than double the size of Jiuzhang 2 by using 127 qubits to solve problems. It is the latest event in a race to build a quantum computing device that can be used for practical applications, spearheaded by Google's announcement of quantum supremacy in 2019 with its Sycamore processor, which utilizes the same superconducting architecture as IBMs new Eagle processor and China's Jiuzhang 2.

The term quantum supremacy refers to the successful achievement of a calculation, by a quantum computer, that it would be impossible for a classical computer to achieve. IBM has previously contested Google's assertion that it reached quantum supremacy, saying that the search firm greatly exaggerated the difficulty of the tasks its Sycamore computer completed.

Quantum computing can 'tackle the biggest problems of our time’

IBM's 127-qubit Eagle processor is now, theoretically speaking, the most powerful quantum computer in the world, though it is yet to be put through its paces. Unlike Google and China's USTC, IBM hasn't published an academic paper detailing tests conducted on its quantum computer to demonstrate its performance. Qubits count is also not the be all and end all when it comes to quantum computing power. The Jiuzhang 2, for example, had a total of 66 qubits, and it was 10 million times faster than Google's 54-qubit Sycamore, due, in part, to its use of light photons.

Still, IBM points an impressive statistic about Eagle in its statement. The company claims that the number of classical computing bits required to represent a state on its new Eagle processor would be larger than the number of atoms in the entire living human population of roughly 7.5 billion people.

"Quantum computing has the power to transform nearly every sector and help us tackle the biggest problems of our time," said Dr. Darío Gil, Senior Vice President, IBM and Director of Research. "The arrival of the Eagle processor is a major step towards the day when quantum computers can outperform classical computers for useful applications," he continued.

IBM revealed a quantum computing roadmap last year in which it revealed its plans to demonstrate a 400-qubit processor next year, before building a 1000-qubit quantum computing chip called Condor by 2024.

16.QuEra Computing has built a record-breaking 256-qubit quantum computer

by Siobhan Roberts
https://www.technologyreview.com/2021/11/17/1040243/quantum-computer-256-bit-startup/

At long last, physicists from Harvard and MIT have found the killer application for quantum computing: a Mario Bros. The qubits can also be arranged in a Space Invaders design, or Tetris, or any other shape—your geometrical wish is the qubits' command.

The GIFs were offered up by QuEra Computing, a Boston startup emerging from stealth, to show off the programmability of their 256-qubit quantum simulator—a special-purpose quantum computer built for solving certain types of problems.

The QuEra machine is the latest leap in scaling up quantum computing to make it more powerful and capable of tackling practical problems. More qubits mean more information can be stored and processed, and researchers developing the technology have been racing to continually raise the bar.

In 2019, Google announced that its 53-qubit machine had achieved quantum supremacy—performing a task not manageable by a conventional computer—but IBM challenged the claim. The same year, IBM launched its 53-bit quantum computer. In 2020, IonQ unveiled a 32-qubit system that the company said was the "world's most powerful quantum computer." And just this week IBM launched its new 127-qubit quantum processor, which the press release described as a "minor miracle of design." "The big news, from my perspective, is it works," says Jay Gambetta, IBM's vice-president of quantum computing.

Now QuEra claims to have made a device with far more qubits than any of those rivals.

The ultimate goal of quantum computing, of course, is not to play Tetris but to outperform classical computers in solving problems of practical interest. Enthusiasts reckon that when these computers become powerful enough, perhaps in a decade or two, they might bring transformative effects in fields such as medicine and finance, neuroscience and AI. Quantum machines will likely need thousands of qubits to manage such complex problems.

The number of qubits, however, is not the only factor that matters.

QuEra is also touting the enhanced programmability of its device, in which each qubit is a single, ultra-cold atom. These atoms are precisely arranged with a series of lasers (physicists call them optical tweezers). Positioning the qubits allows the machine to be programmed, tuned to the problem under investigation, and even reconfigured in real time during the computation process.

"Different problems are going to require the atoms to be placed in different configurations," says Alex Keesling, QuEra's CEO and co-inventor of the technology. "One of the things that's unique about our machine is that every time we run it, a few times a second, we can completely redefine the geometry and the connectivity of the qubits."

The atom advantage

QuEra's machine was built from a blueprint and technologies refined over several years, led by Mikhail Lukin and Markus Greiner at Harvard and Vladan Vuletić and Dirk Englund at MIT (all are on QuEra's founding team). In 2017, an earlier model of the device from the Harvard group used only 51 qubits; in 2020, they demonstrated the 256-qubit machine. Within two years the QuEra team expects to reach 1,000 qubits, and then, without changing the platform much, they hope to keep scaling up the system beyond hundreds of thousands of qubits.

It's QuEra's unique platform—the physical way that the system is assembled, and the method by which information encoded and processed—that should allow for such leaps of scale.

While Google's and IBM's quantum computing systems use superconducting qubits, and IonQ uses trapped ions, QuEra's platform uses arrays of neutral atoms that produce qubits with impressive coherence (that is, a high degree of "quantumness"). The machine uses laser pulses to make the atoms interact, exciting them to an energy state—a "Rydberg state," described in 1888 by the Swedish physicist Johannes Rydberg—at which they can do quantum logic in a robust way with high fidelity. This Rydberg approach to quantum computing has been worked on for a couple of decades, but technological advances—for instance, with lasers and photonics—were needed to make it work reliably.

"Irrationally exuberant"

When the computer scientist Umesh Vazirani, director of the Berkeley Quantum Computation Center, first learned about Lukin's research along these lines, he felt "irrationally exuberant"—it seemed like a marvelous approach, though Vazirani questioned whether his intuitions were in touch with reality. "We've had various well-developed paths, such as superconductors and ion traps, that have been worked on for a long time," he says. "Shouldn't we be thinking about different schemes?" He checked in with John Preskill, a physicist at the California Institute of Technology and the director of the Institute for Quantum Information and Matter, who assured Vazirani that his exuberance was justified.

Preskill finds Rydberg platforms (not just QuEra's) interesting because they produce strongly interacting qubits that are highly entangled—"and that's where the quantum magic is," he says. "I'm pretty excited about the potential on a relatively short time scale to discover unexpected things."

In addition to simulating and understanding quantum materials and dynamics—which Lukin calls "the first examples of useful quantum advantage involving scientific applications"—the researchers are also working on quantum algorithms for solving computational optimization problems that are NP-complete (that is, very hard).

One of QuEra's investors is Rakuten, a Japanese internet services, e-commerce, and fintech company, which is interested in exploring the problem of optimizing antenna locations for 4G and 5G mobile services. "Also, the technology has promise for solving many optimization problems from delivery routing, stock portfolio, search engines to recommendations," says Takuya Kitagawa, Rakuten's chief data officer. "The dream is big."

Preskill, however, isn't particularly optimistic that QuEra's machine will outperform classical algorithms for optimization problems. He's the one who coined the term quantum supremacy (describing the point at which quantum computers can do things that classical computers can't), and he notes: "We don't have strong theoretical arguments that we'll see quantum advantage in optimization any time soon. But it is certainly worthy of investigation."

And Preskill is keen on QuEra’s plan to make its platform widely accessible for research and development. Having a larger community of people fooling around and playing with the machines, he says, will help to figure out what they’re good at. Hopefully, they won’t spend their time just playing Tetris and Space Invaders.

17.IQM Quantum Computer Will Be First Quantum System to be Integrated into a HPC Supercomputer

by Matt Swayne
https://thequantuminsider.com/2021/11/17/q-exa-collaborative-iqm-quantum-computer-will-be-first-quantum-system-to-be-integrated-into-a-hpc-supercomputer/

IQM Quantum Computers has been selected to provide a quantum computing system that will be integrated into an HPC supercomputer to create an accelerator for future scientific research. The delivery is part of a €45.3 million consortium project. The project is funded by the German Federal Ministry of Education and Research (BMBF) with €40.1 million.

The highly interdisciplinary consortium with experts from quantum physics and computer science, from research centers and industry, will integrate a quantum computing system provided by IQM into an HPC environment via a research purchase. This will be the first time that a gate-based quantum system will be coupled with an HPC system, making quantum acceleration of HPC applications a reality.

Quantum computers have significant potential for solving a certain class of scientific and industrial problems that cannot be addressed by classical supercomputers. To meet this challenge, HPC centers around the world are looking for ways to integrate quantum accelerators into their computing infrastructure. The ability to provide on-site solutions for quantum computing in conjunction with supercomputers is essential for the development of cutting-edge high-tech solutions from Europe. The main goal of the Q-Exa project is to establish such solutions and thus strengthen the application-related use of quantum technologies from Germany.

IQM will work with Leibniz Supercomputing Centre, LRZ – one of Germany’s three national supercomputing centers, Europe´s leading HPC and quantum system provider (Atos) and one of Germany’s leading innovators of quantum computing applications (HQS) on this project.

Q-Exa´s collaborative approach creates strong synergies with other research projects in the German and European ecosystem. The previously announced BMBF project DAQC benefits from novel simulators and fits seamlessly into the concept of the Q-Exa Co-Design Lab. The new Co-Design lab will accelerate the path to self-sustaining quantum computing, the so-called quantum advantage, through industry partnerships. This approach is in line with other German industry efforts, such as the recently formed QUTAC consortium. On the application side, research consortia such as the BMBF projects QLindA, MANIQU and other initiatives support development as industrial use cases can be tested on the Q-Exa demonstrators. Finally, the Q-Exa project supports the European strategy based on integrating quantum computing accelerators into European HPC centers. With Q-Exa, Germany can make an active contribution to these European efforts.

Federal Research Minister Anja Karliczek says: “The international race in the field of quantum technologies is in full swing. Germany and the European Union must do their utmost to keep pace in order to guarantee our technological sovereignty. We want to be able to autonomously use the technology and develop it further. The Q-Exa project opens a new promising chapter on our path to a quantum computer ‘made in Germany’. Integrating a quantum computer with the infrastructure of the Leibniz Supercomputing Centre harbours enormous potential for science and industry. The project will contribute to bringing quantum computers close to practice and to provide specific application scenarios for users in science and industry. I am delighted that by launching the project we have reached the first milestone on the way towards a competitive quantum computer ‘made in Germany’.”

Dr. Jan Goetz, CEO of IQM Quantum Computers remarks: “We are pleased to deliver a quantum computing system to LRZ and to work with the consortium partners to integrate this system into a production-grade HPC environment. I am grateful to the Federal Ministry of Education and Research in Germany, which has given us the necessary trust and support for this ambitious project. Together we will work hard to make European technology competitive and develop the most promising hardware solutions for quantum computing here in Germany”.

Prof. Dr. Dieter Kranzlmüller, Chairman of the Board of Directors, LRZ, points out: “The Q-Exa project is key for our activities within the LRZ Quantum Integration Centre (QIC) and the Munich Quantum Valley (MQV). Working with this extremely competitive consortium, we will be able to set European standards that are competitive on a global scale. Ultimately, this will be for the benefit of society as the integration of quantum computing into supercomputers, in particular on the exascale level, will speed up and open vast new research possibilities. It will bring quantum computing to users – both in academia and in industry. And now is exactly the right time to realize this in a data center environment”.

“Technological sovereignty in strategic areas like quantum computing is critical for Europe. With our Quantum Learning Machine (QLM) and strong startup partners like IQM, Atos is proud to contribute to this joint effort. It is time to build the first German quantum computer, connected to an HPC datacenter through our QLM”, says Udo Littke, Head of Atos Central Europe.

“Quantum computers will accelerate scientific progress and the development of new technologies in many areas. Chemistry, physics and biology can potentially profit from the ability to perform improved quantum mechanical simulations. Therefore, it is the next logical step to integrate quantum computers into high performance computer centers like the LRZ. We are looking very much forward to connect the end users of the LRZ with the necessary software tools to make full use of the coming computational capabilities”, says Dr. Michael Marthaler, CEO HQS Quantum Simulations GmbH.

18.The Unknown Unknowns: Tales from The Crypto Crypt

by Mike Brown

https://www.forbes.com/sites/forbestechcouncil/2021/11/16/the-unknown-unknowns-tales-from-the-crypto-crypt/?sh=28959af04859&utm_medium=email&_hsmi=188845838&_hsenc=p2ANqtz-9qxLKXpNkRK-0eaVltbpmDK6My_8Dpvc0Ad0Do1FcBQPU9lY4m5JuTdN-L1DZJON7t6EJ90rVOjYhUvQB0gJj51vifRA&utm_content=188845838&utm_source=hs_email

Slime oozing. Skeletons dangling. Spiderwebs hanging. Zombies chasing. These could be scenes from any scary movie or from the classically creepy TV series *Tales from the Crypt*, where the Cryptkeeper pops out of his coffin to introduce stories about monsters, the supernatural and everyday horrors.

Speaking of everyday horrors...what about crypto lurking? In today’s connected ecosystems, broken cryptography makes the perfect plot for the scariest of movies. Unauthorized access to sensitive information, damage to critical infrastructure, lost control over devices and data — all of it equates to mayhem.

Any threat to cryptography is a threat to be taken seriously. Even more so now, with the looming quantum threat ahead. The question is not whether quantum computers will render the classic public-key cryptography obsolete but what each enterprise will do when the new public-key cryptographic standards are released by the National Institute of Standards and Technology (NIST), which NIST has indicated could be as early as 2022.

Since the dawn of the internet, cryptography has been at the core of every secure transaction. It usually hums along in the background, working its security magic across protocols, inside hardware and behind applications. Cryptography is the foundation of digital trust: authentication, authorization, confidentiality and data integrity. As the enabler of overall enterprise security, public-key cryptography ensures the protection and authenticity of all transactions and participants in the digital world.

The emerging quantum threat brings cryptography management to the forefront, with boards asking their CISOs what their plan of action is. There is now more reason why these mission-critical assets, systems and data all require the utmost attention, management and protection.

What Crypto Is Lurking In Your Basement? What You Don’t Know Can Hurt You

Generally, organizations don’t have a good handle on the location of all the cryptography deployed throughout their infrastructure — or how healthy it is. The number of devices, systems and technologies used within enterprises that use cryptography continues to rapidly grow and shows no signs of slowing down. Almost every application and IT system contain cryptography, found throughout all the various layers of an organization’s infrastructure — whether on-premises or in the cloud. This makes it increasingly difficult for organizations to shine a light on their cryptographic assets.

Your organization may not be doing business in a decrepit mansion and your cryptography may not be housed deep in a dark basement (or maybe it is?). But maybe it’s in your organization’s server room, in the cloud, on devices and in third-party applications. Within organizations, there is often a lack of insight into where cryptography resides, centralized management and enforcement of crypto governance, and a lack of efficient cryptographic audit capabilities.

Why Prioritize Cryptographic Management: Thoughts From A ‘Crypto-Keeper'

To reduce risks, cryptographic infrastructures need to be visible. The critical first step is gaining visibility into your cryptography: inspect what you cannot see. Tracking and inventorying cryptography used across the enterprise will be helpful to engage the C-suite and the board and start building corporate migration plans. By prioritizing crypto agility — the ability to migrate between crypto standards without the business disruption and in a cost-effective way — the stress of cryptographic migrations will lessen.

With insight into an enterprise’s cryptography, those responsible can build the case for more resources and funding for cryptographic upgrades and migration through audits and executive reports. “Having the visibility necessary to reduce risk is one of the most critical parts of security. ... A single view across the battlefield is vital,” states Uri Levy, SVP global strategy, XM Cyber, in an *Infosecurity Magazine* article on the importance of identifying and defending your organization’s crown jewels. Some early movers have even created a cryptography center of excellence (CCoE) to raise the profile of crypto heath and to carve out the importance of making crypto insight a priority.

Health.com’s Patti Greco outlines reasons why we love horror movies: They give you a thrilling rush, help you prepare for the worst and teach you to cope. These lessons can be applied to cryptographic management: get started, prepare, cope. But don’t let the unknown scare you. While organizations’ cryptography may be lurking, there’s no such thing as crypto monsters. With crypto-agile processes and tools and the right cryptographic management planning in place, organizations can be in control of their cryptography and future-proof what's ahead.

19.How Quantum Computers Will Correct Their Errors

by Katie McCormick

https://www.quantamagazine.org/how-quantum-computers-will-correct-their-errors-20211116/

In 1994, Peter Shor, a mathematician then at Bell Labs in New Jersey, proved that a quantum computer would have the power to solve some problems exponentially faster than a classical machine. The question was: Could one be built? Skeptics argued that quantum states were too delicate — the environment would inevitably jumble the information in the quantum computer, making it not quantum at all.

A year later, Shor responded. Classical error-correcting schemes measured individual bits to check for errors, but that approach wouldn't work for quantum bits, or "qubits," since any measurement would destroy the quantum state, and hence the calculation. Shor figured out a way to detect whether an error had occurred without measuring the state of the qubit itself. Shor's code marked the beginning of the field of quantum error correction.

The field has flourished. Most physicists see it as the only path to building a commandingly powerful quantum computer. "We won't be able to scale up quantum computers to the degree that they can solve really hard problems without it," said John Preskill, a physicist at the California Institute of Technology.

As with quantum computing in general, it's one thing to develop an error-correcting code, and quite another to implement it in a working machine. But at the beginning of October, researchers led by Chris Monroe, a physicist at the University of Maryland, reported that they had demonstrated many of the ingredients necessary to run an error-corrected circuit like Shor's.

So how did Shor crack the conundrums he faced? He used the added complexity of quantum mechanics to his advantage.

Repeat Repeat Repeat

Shor modeled his protocol after the classical repeater code, which involves making copies of each bit of information, then periodically checking those copies against each other. If one of the bits is different from the others, the computer can correct the error and continue the calculation.

Shor designed a quantum version of this. He used three individual "physical" qubits to encode a single qubit of information — the "logical" qubit. Shor's quantum repeater code couldn't be exactly the same as the classical version, though. The essential power of quantum computation comes from the fact that qubits can exist in a "superposition" of being in a combination of 0 and 1 at the same time. Since measuring a quantum state would destroy the superposition, there wasn't a straightforward way to check to see whether an error had occurred.

Instead, he found a way to tell if the three physical qubits were in the same state as one another. If one of the qubits was different, it would indicate that an error had occurred.

The task is not unlike solving a simple logic puzzle. You're given three balls that look identical, but one of the balls might have a different weight. You also have a simple balance scale. What measurements will let you determine whether there is an oddball in the mix, and if so, which one it is?

The answer is to first pick two balls and compare their weights, then replace one of the balls with the remaining ball and check again. If the scale was balanced both times, then all balls are identical. If it was balanced only once, then one of the replaced balls is the odd one out. If the scales are imbalanced both times, the ball that stayed still is the culprit.

Shor's code replaces the scales with two extra "ancilla" qubits. The first of these compares the first and second physical qubits; the other compares the second and third. By measuring the states of these ancillary qubits, you learn if the three information-containing qubits are in identical states without disturbing the state of any of them.

This code protects against a bit flip, which is the only possible error that can occur in classical computing. But qubits have one more potential source of error.

Superpositions are the key to quantum computing, but it's not just the value of the qubit that's important. The relative "phase" between qubits matters too. You can think of this phase as a wave — it tells you the location of the wave's peaks and troughs. When two waves are in phase, their ripples are synchronized. If they collide, they will constructively interfere, merging into a single wave double the size. But if the waves are out of phase, then when one wave is at its peak, the other is at its nadir, and they will cancel each other out.

A quantum algorithm takes advantage of this phase relationship among its qubits. It sets up a situation where the correct answer to a calculation constructively interferes and is therefore amplified, while the incorrect answer gets suppressed by destructive interference.

But if an error causes the phase to flip, then destructive interference can switch to constructive interference, and the quantum computer will start amplifying the wrong answer.

Shor found that he could correct for phase errors using a similar principle to the one he used for bit flips. Each logical qubit gets encoded into three qubits, and ancilla qubits check to see if one of the phases has flipped.

Shor then combined the two codes. The result was a code that translated one logical qubit into nine physical qubits that offered both bit and phase checks.

Tolerant to a Fault

Shor's code would in principle protect a single logical qubit from errors. But what if there was a mistake in the error measurements themselves? Then, in your attempt to correct the nonexistent error, you would flip a bit and unwittingly introduce a real error. In some cases, this could cause a cascade of errors to propagate through the code.

Shor's code also didn't consider how he would operate a quantum computer built from his logical qubits. "We need some way to do computations on the encoded states, without losing that protection. And that's not straightforward," said Daniel Gottesman, a theoretical computer scientist at the University of Maryland.

So in 1996, his third consecutive year of blazing trails, Shor came up with the notion of fault tolerance. A fault-tolerant code can deal with errors introduced by the environment, by imperfect operations on those qubits, and even by the error-correction steps themselves — provided the rate at which these errors occur is below a certain threshold.

Last month, Monroe and his group announced that they had used a fault-protected version of Shor's code called the Bacon-Shor code to demonstrate nearly all the tools necessary for a fully fault-tolerant quantum computer. They encoded a logical qubit into the quantum states of nine ions, then, using four ancilla qubits, they showed that they could fault-tolerantly perform all single-qubit operations necessary for quantum computing. The result shows that a fault-tolerant quantum computer is possible.

This goal remains distant, though. Monroe thinks the advantage granted by error correction won't be seen until quantum computers have reached about 100 logical qubits. Such a machine would require about 1,300 physical qubits, since each logical qubit needs nine physical qubits plus four ancillas. (The current largest quantum processor, IBM's newly announced Eagle, has 127 physical qubits.) At that point, "we're going to start making a qubit factory and then we'll introduce error correction," said Monroe. "But not before."

20.IBM debuts quantum machine it says no standard computer can match

by Julien Levallois

https://www.swissquantumhub.com/ibm-debuts-quantum-machine-it-says-no-standard-computer-can-match/

IBM has announced its largest quantum processor to date, as the company seeks to show it is on track to create a commercially-useful quantum computer by the end of 2023.

The new quantum hardware, which IBM is calling Eagle, has 127 qubits, which are the information-processing units of a quantum computer. This is a large enough cluster to perform calculations that cannot be made by traditional computers in a reasonable timeframe, the company said.

But the company said it had not yet done a benchmark demonstration to prove that the new processor can perform tasks beyond the grasp of conventional computers, saying only that the new machine is powerful enough that it should be able to do so.

Quantum computers are machines that use phenomena from quantum physics to process information. In a traditional computer, information is represented in a binary form, known as a bit. A bit can be either a zero or one. In a quantum computer, information is represented by a quantum bit, or qubit for short, that can be placed into a quantum state in which it can represent both zero and one at the same time.

Also, in a classical computer, all the bits in a computer chip function independently. In a quantum computer, the qubits are "entangled" with others in the quantum processor, enabling them all to work together to reach a solution. Those two properties give quantum computers, in theory, exponentially more power than a traditional computer.

But to date, quantum computers have been too underpowered—meaning they have too few qubits and those qubits cannot remain in a quantum state long enough—to pose a major challenge to traditional computers. In 2019, Google achieved a milestone called "quantum supremacy" in which it performed a simulation of a quantum physics problem that could not be carried out on a traditional computer. But, as important as that achievement was in the annals of computer science, it did not have any immediate business applications.

Quantum leap

There are two main problems holding back today's quantum computers: they don't have enough qubits in most cases to perform calculations that would give them an edge on standard computers. What's more, those qubits can only remain in a quantum state for very short periods of time (often just a few hundred microseconds.) And when the qubits fall out of a quantum state, errors creep into their calculations. These errors need to be corrected, either by using more qubits, or by using software, but exactly how to do so efficiently remains an unsolved problem.

IBM last year unveiled a roadmap for the emerging technology that would see the company producing a quantum processor with more than 400 qubits by the end of next year and one with at least 1,000 qubits by 2023. A quantum computer of that size ought to be able to perform many useful business applications, the company has said.

The company is one of dozens around the world racing to commercialize quantum technology. Other leading contenders including tech titan Google, and industrial giant Honeywell, which recently spun off its quantum computing division into a separate public company, as well as D-Wave Systems, Rigetti Computing, and IonQ. Microsoft also has a quantum computing effort, although it has suffered setbacks.

IBM's Eagle processor has almost two times the number of qubits as the company's previous largest quantum processor, the 65-qubit Hummingbird, that it debuted last year.

Jerry Chow, the manager of IBM's experimental quantum group, said that the company was still working to benchmark the performance of the new Eagle processor. He said the company still was not ready to say how long the Eagle's qubits can remain in a quantum state or the degree to which the qubits are entangled.

He also said that IBM was debuting a new metric for measuring quantum performance called circuit layer operations per second, or CLOPS for short. This stat matters because a quantum computer does not produce a single, accurate result for a calculation, as a classical computer does. Instead, the answer can vary each time the calculation is run. As a result, to reach an accurate solution, the same calculation needs to be run through the quantum processor hundreds or even thousands of times, with the distribution of results converging over time on an accurate solution. In other words, if you ran the same calculation 100 times, and 85 times it produced answer A, then A is the accurate solution, even though 15 times the quantum computer spat out answer B.

But Chow said IBM was not yet ready to release a CLOPS figure for the new Eagle processor. "This is again an area where we are in process of measuring," he told Fortune.

Chow also said that IBM is making progress in increasing the coherence times of its earlier 27-qubit Falcon processor. It said the qubits in this processor could now remain in a quantum state for as long as 300 microseconds, about three times the median rate for most other qubits built using superconducting materials like IBM's. (Other companies are pursuing different methods of creating qubits, including using lasers to trap ions, and using silicon-based processors, similar to the materials used in standard computer chips, to create qubits.)

The new Eagle processor will be accessible through a cloud-based connection to companies that are part of IBM's Q Network of early quantum adopters by the end of the year. Most of these companies, which include the likes of Toyota, Wells Fargo and Delta Airlines, have been experimenting with quantum computers and running small proof of concept projects, but have not deployed quantum computers into any real business units.

21.Creating Dynamic Symmetry in Diamond Crystals to Improve Qubits for Quantum Computing

by MATTHEW HUTSON
https://scitechdaily.com/creating-dynamic-symmetry-in-diamond-crystals-to-improve-qubits-for-quantum-computing/

Physicists and engineers have long been interested in creating new forms of matter, those not typically found in nature. Such materials might find use someday in, for example, novel computer chips. Beyond applications, they also reveal elusive insights about the fundamental workings of the universe. Recent work at MIT both created and characterized new quantum systems demonstrating dynamical symmetry — particular kinds of behavior that repeat periodically, like a shape folded and reflected through time.

“There are two problems we needed to solve,” says Changhao Li, a graduate student in the lab of Paola Cappellaro, a professor of nuclear science and engineering. Li published the work recently in Physical Review Letters, together with Cappellaro and fellow graduate student Guoqing Wang. “The first problem was that we needed to engineer such a system. And second, how do we characterize it? How do we observe this symmetry?”

Concretely, the quantum system consisted of a diamond crystal about a millimeter across. The crystal contains many imperfections caused by a nitrogen atom next to a gap in the lattice — a so-called nitrogen-vacancy center. Just like an electron, each center has a quantum property called a spin, with two discrete energy levels. Because the system is a quantum system, the spins can be found not only in one of the levels, but also in a combination of both energy levels, like Schrodinger’s theoretical cat, which can be both alive and dead at the same time.

The energy level of the system is defined by its Hamiltonian, whose periodic time dependence the researchers engineered via microwave control. The system was said to have dynamical symmetry if its Hamiltonian was the same not only after every time period t but also after, for example, every t/2 or t/3, like folding a piece of paper in half or in thirds so that no part sticks out. Georg Engelhardt, a postdoc at the Beijing Computational Science Research, who was not involved in this work but whose own theoretical work served as a foundation, likens the symmetry to guitar harmonics, in which a string might vibrate at both 100 hertz and 50 Hz.

To induce and observe such dynamical symmetry, the MIT team first initialized the system using a laser pulse. Then they directed various selected frequencies of microwave radiation at it and let it evolve, allowing it to absorb and emit the energy. “What’s amazing is that when you add such driving, it can exhibit some very fancy phenomena,” Li says. “It will have some periodic shake.” Finally, they shot another laser pulse at it and measured the visible light that it fluoresced, in order to measure its state. The measurement was only a snapshot, so they repeated the experiment many times to piece together a kind of flip book that characterized its behavior across time.

“What is very impressive is that they can show that they have this incredible control over the quantum system,” Engelhardt says. “It’s quite easy to solve the equation, but realizing this in an experiment is quite difficult.”

Critically, the researchers observed that the dynamically symmetry of the Hamiltonian — the harmonics of the system’s energy level — dictated which transitions could occur between one state and another. “And the novelty of this work,” Wang says, “is also that we introduce a tool that can be used to characterize any quantum information platform, not just nitrogen-vacancy centers in diamonds. It’s broadly applicable.” Li notes that their technique is simpler than previous methods, those that require constant laser pulses to drive and measure the system's periodic movement.

One engineering application is in quantum computers, systems that manipulate qubits, bits that can be not only 0 or 1, but a combination of 0 and 1. A diamond's spin can encode one qubit in its two energy levels.

Qubits are delicate: they easily break down into simple bit, a 1 or a 0. Or the qubit might become the wrong combination of 0 and 1. "These tools for measuring dynamical symmetries," Engelhardt says, "can be used to as a sanity check that your experiment is tuned correctly — and with a very high precision." He notes the problem of outside perturbations in quantum computers, which he likens to a de-tuned guitar. By tuning the tension of the strings — adjusting the microwave radiation — such that the harmonics match some theoretical symmetry requirements, one can be sure that the experiment is perfectly calibrated.

The MIT team already has their sights set on extensions to this work. "The next step is to apply our method to more complex systems and study more interesting physics," Li says. They aim for more than two energy levels — three, or 10, or more. With more energy levels they can represent more qubits. "When you have more qubits, you have more complex symmetries," Li says. "And you can characterize them using our method here."

22.Can Europe compete in the quantum 'space race'?

by Alice Pannier
https://techcrunch.com/2021/11/14/can-europe-compete-in-the-quantum-space-race/

The TechCrunch Global Affairs Project examines the increasingly intertwined relationship between the tech sector and global politics.

Quantum information science has long languished in an academic corner of the tech sector. But recent advances mean that the sector has taken on geopolitical significance. With several nations rushing to develop their own quantum systems, the quantum competition has started to resemble a new "space race."

With the U.S. and China leading the way, European countries are feeling the pressure to step up their game, and several countries, as well as the European Union itself, have made a big push to invest in this space. But are European efforts too late and too fragmented to compete with the two tech giants?

U.S.-China: A race to the quantum advantage and beyond

Quantum computing seeks to exploit the counter-intuitive properties of quantum physics (that is to say, physics at the atomic or subatomic scale), such as entanglement and superposition. To do so, a quantum computer manipulates the states of particles (ions, electrons, photons) using lasers or electric and magnetic fields.

The United States and China have the most advanced quantum capabilities, with both claiming to have reached "quantum supremacy," i.e., the ability to solve mathematical problems that would take a classical computer millions of years.

China's efforts have been ongoing since around 2015, when the Edward Snowden revelations prompted anxiety over the extent of U.S. intelligence activities. Anxious about American capabilities, Beijing intensified its focus on quantum communications. Estimates of China's spending on quantum research vary, but the country is the leading holder of patents in quantum communication and cryptography hardware and software. Chinese efforts in quantum computers are more recent, but Beijing has been moving fast. In December 2020 and again in June 2021, researchers from the University of Science and Technology of China (USTC) made credible claims to have achieved "quantum supremacy."

Washington woke up to the possibility of China's lead in quantum technologies when Beijing demonstrated its capacity in satellite-based quantum communications in 2016. In response, then-President Donald Trump launched a $1.2 billion National Quantum Initiative in 2018. Meanwhile — and perhaps most importantly — big technology firms started pouring huge sums into their own quantum research. IBM, which introduced the first two-qubit computer in the 1990s, is now exporting its Quantum System One machine. Though newer to the field, Google claimed to have achieved quantum supremacy in 2019 with a 53-qubit quantum processor based on superconductors.

Technologies with geopolitical implications

Driving China, the U.S. and other countries is a fear that lagging behind in quantum computing will pose cybersecurity, technological and economic risks.

First, a fully functioning quantum computer could allow an adversary to break any public encryption key currently in use. While it would take a classical computer 300 trillion years to crack a 2,048-bit RSA encryption key (used to secure online payments), a quantum computer with 4,000 stable qubits could in theory do the same in just 10 seconds. Such technology could be less than a decade away.

Second, European governments fear the consequences of becoming caught between American and Chinese quantum competition. Chief among those is quantum tech becoming subject to export restrictions. These should be coordinated among allied countries. Europeans remember how the U.S. embargoed the export of state-of-the-art computer equipment to France during the Cold War for fear that the technology could fall into Soviet hands. This motivated France to develop and support a national supercomputer industry.

Today, America's European partners are concerned that in a tech cold war, they may struggle to access critical technologies or trade technologies with third countries. In addition to expanding its list of controlled items, the U.S. is adding more and more Chinese organizations to the "Entity List" (e.g., Chinese supercomputing centers in April 2021), thereby blocking technology exports — including from non-U.S. companies — to those entities. And as the list of restricted technologies grows, European companies feel the financial consequences in their international value chains. In the near future, some enabling technologies needed to make quantum computers work — such as cryostats — could be placed under control too.

But there are concerns about China as well. China has posed other types of risks to countries' technological development, including challenging intellectual property rights and academic freedom, and it is well versed in economic coercion.

A final risk is economic. A disruptive technology like quantum computing will have massive industrial implications. While demonstrating "quantum supremacy" may constitute a scientific show of force, most governments, research labs and startups are in fact seeking to harness the "quantum advantage" — i.e., an acceleration of computing power sufficient to provide an advantage compared to classical machines for practical applications.

Considering its many use cases in complex simulation, optimization and deep learning, quantum computing will likely become a thriving business in the decades to come. Some quantum startups are already starting to go public in what is becoming a quantum investment frenzy. Europeans fear losing out on what stands to be a significant part of the 21st century economy.

Is Europe up to the task?

Unlike in most other digital technologies, Europe is well positioned in the global quantum race.

The U.K., Germany, France, the Netherlands, Austria and Switzerland all have significant quantum research capacities and flourishing startup ecosystems. Their governments, as well as the European Union, are making significant investments in quantum computing hardware and software and in quantum cryptography. In fact, the U.K. launched its National Quantum Technologies Program in 2013, well before the U.S. and China. As of 2021, Germany and France are just behind the U.S. in terms of public investment in quantum research and development, with approximately €2 billion and €1.8 billion, respectively. Amazon is even developing a quantum computer based on a self-correcting quantum bit (qubit) technology discovered by the French hardware startup Alice & Bob.

So, what stands in Europe’s way to become a serious challenger to the U.S. and China?

For one, the challenge for Europe is less fostering the emergence of startups but keeping them. Most promising European startups have a tendency not to grow on the continent due to inadequate venture capital. Europe’s AI successes are a cautionary tale; many recall how Google (Alphabet) acquired DeepMind, one of the most promising British startups. The story is repeating itself with PsiQuantum, a leading British startup, which settled in California in search of capital.

To counter that risk, European governments and the European Union have launched several initiatives in emerging and disruptive technologies with the goal of building European “technological sovereignty.” But then, does Europe even adopt its own technologies? EU procurement rules do not necessarily favor European suppliers in contrast to the U.S. “Buy American Act.” Today, EU member states are reluctant to favor European technology providers when more advanced or cheaper foreign options exist, as Germany recently did with its acquisition of an IBM machine. This may change with the International Procurement Instrument, a new piece of legislation currently being negotiated in Brussels, which would introduce a principle of reciprocity in the openness of public procurement markets.

Alongside the government, private companies will play a key role in shaping the future quantum industry through their choices of investments, partnerships and adoption of technologies. The choice to opt for IBM systems in the 1960s and 1970s has had a lasting effect in structuring the global computing market. Similar choices in quantum computing have the potential to shape the field for decades to come.

The dissatisfaction in Europe today about the scarcity of world-leading European tech firms only underscores the significance that early choices in the support for and adoption of technologies can have. If Europe is to be competitive in quantum with the U.S. and China in the years to come, it must not just maintain its current momentum but increase it.

23.What is Encryption and Why is it Key to Human Rights?

by Verónica Ferrari
https://goodmenproject.com/featured-content/what-is-encryption-and-why-is-it-key-to-human-rights/

Encryption is the process of making messages or files unreadable by anyone except for people who have the key or password to decrypt them. During encryption, a file is encoded in a way that converts the original representation into an alternative form that can only be deciphered (converted back) by authorised parties following a certain procedure and using a key or password. As APC member Open Net Korea says, it is saying something “in a secret language that is known only to a closed group of people.”

Encryption is one of the best techniques that we have to protect information from interference when navigating the internet and in our devices and email. Encryption can be implemented using software applications, special hardware or a combination of both. A stronger form of encryption is end-to-end encryption, which encrypts data even before it is sent to a server. When used correctly, it is virtually impossible (or extremely time consuming) to break with current technologies.

Why is encryption key to human rights?

Encryption is key to preserving confidentiality and anonymity in our online communications, and is therefore essential for the enjoyment of a range of human rights. In its latest resolution on privacy in the digital age, the UN Human Rights Council stressed the importance of encryption, pseudonymisation and anonymity to ensure, in particular, the enjoyment of the rights to privacy, to freedom of opinion and expression, and to freedom of peaceful assembly and association.

In June 2015, the UN Special Rapporteur on freedom of opinion and expression dedicated a report to the fundamental role of encryption for the full exercise of the right to freedom of expression, and examined the ways in which encryption establishes, among other things, a measure of privacy that enables people to use the internet to develop opinions and access information online without interference. The report also explores how anonymity is linked to the right to privacy and explains that “an individual cannot have a reasonable expectation that his or her privacy is being protected without the ability to control what information is shared about them and how that information is used.”

As APC has emphasised, anonymity is also inextricably linked to the right to privacy. And the lack of privacy, or even the perception of the lack of privacy, can have a chilling effect on freedom of expression and lead to self-censorship.

The mandate of the United Nations Special Rapporteur on freedom of peaceful assembly and association has also addressed the importance of encryption providing a safe online space to gather, connect, organise and coordinate activities, without undue interference from third parties and governments.

Encryption is also connected with self-determination and the ways in which we occupy digital spaces. APC member May First Movement Technology considers encryption to be a key part of “the struggle to regain democratic and community ownership of our data and technology infrastructure and development itself.”

As we stated in our explainer on cybersecurity, weakened encryption undermines human rights: it can make it easier for malicious actors to gain access to people's personal information and communications, can lead to journalists' sources being revealed, human rights defenders being targeted by governments, and a person in an abusive relationship being blackmailed. Encryption and anonymity provide the privacy and security necessary for the exercise of a range of rights and should be strengthened.

Why does encryption especially matter for women and people of diverse gender and sexual expressions?

Women and people of diverse gender and sexual expressions are especially vulnerable to violations of privacy, since their experiences take place within a context of existing structural inequalities and discrimination that put them at particular risk of violence and other types of human rights violations. Therefore, encryption and anonymity are essential tools to empower and protect groups at risk, specifically sexual and gender rights activists and those who are targets of online violence.

The United Nations High Commissioner for Human Rights noted in a report from 2017 that women's right to privacy implies the ability to benefit from encryption and anonymity "in order to minimize the risk of interference with privacy, which is especially pertinent for women human rights defenders and women trying to obtain information otherwise considered taboo in their societies." In her soon to be officially launched new report on gender justice and freedom of expression, Irene Kahn, the UN Special Rapporteur on freedom of expression, states that anonymity and encryption "are an essential facet of women's enjoyment of freedom of opinion and expression in the online context and must be protected."

Anonymity is an important enabler of the right to be free from discrimination, since it enables individuals and minority groups, among others, to associate on sensitive matters such as sexual orientation. Anonymity and encryption are also tools to combat hate speech and online violence and to empower the expression and realisation of sexual rights, as APC has stressed.

It is also important to note that the use of encryption is not only essential to protect human rights online, but also offline, due to the continuum between the online and offline spheres. Groups at risk face consequences that are not solely related to their online interactions and communications, but also have implications for their lived realities. Restrictions to encryption can endanger the physical integrity and life of specific groups at risk.

Finally, APC's Feminist Principles of the Internet explain that anonymity on the internet enables freedom of expression online, particularly when it comes to breaking taboos of sexuality and heteronormativity and experimenting with gender identity, and provides a safe space for women and queer persons affected by discrimination.

What should states and companies do about it?

Many states (and companies) have implemented or proposed measures to weaken encryption tools. For example, through the inclusion of "backdoors" in products, they can bypass the strongest protection and have unlimited access to seemingly secured information. The so-called backdoors can lead to journalists' sources being revealed, human rights defenders and their networks being targeted, or a person in an abusive relationship being blackmailed. As former UN Special Rapporteur on freedom of expression David Kaye said in his report of 2015: "Requiring encryption back-door access, even if for legitimate purposes, threatens the privacy necessary to the unencumbered exercise of the right to freedom of expression."

Countries around the world have also put in place legal bans on the use of encryption of communications, in the name of security and law enforcement. Research by APC member CIPESA found that in Africa, many countries have passed legislation that limits anonymity and the use of encryption through criminalisation of possession and use of cryptographic software or hardware. These trends are accompanied by an increasing persecution of digital security researchers and technical experts who identify and report on vulnerabilities in digital systems to benefit the public at large, such as the case of Ola Bini in Ecuador.

As the UN Special Rapporteur on freedom of expression recommended, states should promote strong encryption and anonymity and should refrain from these measures that interfere with the use of such technologies. Additionally, as APC has said in the past, states should also put in place effective mechanisms for remedy that protect individuals whose rights have been violated due to limitations on anonymity, particularly for individuals from groups at risk.

Companies developing digital services and products have the responsibility to respect human rights, as established by the UN Guiding Principles on Business and Human Rights. Therefore, businesses as well as states should refrain from blocking or limiting the transmission of encrypted communications and, as the UN Human Rights Council stressed, work towards enabling encryption technologies.

In the words of Natasha Msonza, co-founder and chief operations officer of the Digital Society of Africa (DSA) and an APC individual member, "governments and companies should in fact especially be actively promoting and using encryption themselves," as there are malicious actors after their data, too.

Make the switch: Global Encryption Day

Encryption and anonymity-enhancing technologies are essential for the full realisation of the right to privacy, to be free from discrimination, and for the exercise of the freedoms of expression and of association and assembly, among other rights. Proposals for backdoor access, laws that criminalise the use of these tools, and the persecution of digital security experts, among other measures, pose threats to these rights.

24.Cryptocurrency faces a quantum computing problem

by Stephen Shankland

https://www.cnet.com/personal-finance/crypto/cryptocurrency-faces-a-quantum-computing-problem/

Cryptocurrencies hold the potential to change finance, eliminating middlemen and bringing accounts to millions of unbanked people around the world. Quantum computers could upend the way pharmaceuticals and materials are designed by bringing their extraordinary power to the process.

Here's the problem: The blockchain accounting technology that powers cryptocurrencies could be vulnerable to sophisticated attacks and forged transactions if quantum computing matures faster than efforts to future-proof digital money.

Cryptocurrencies are secured by a technology called public key cryptography. The system is ubiquitous, protecting your online purchases and scrambling your communications for anyone other than the intended recipient. The technology works by combining a public key, one that anyone can see, with a private key that's for your eyes only.

If current progress continues, quantum computers will be able to crack public key cryptography, potentially creating a serious threat to the crypto world, where some currencies are valued at hundreds of billions of dollars. If encryption is broken, attackers can impersonate the legitimate owners of cryptocurrency, NFTs or other such digital assets.

"Once quantum computing becomes powerful enough, then essentially all the security guarantees will go out of the window," Dawn Song, a computer security entrepreneur and professor at the University of California, Berkeley, told the Collective[i] Forecast forum in October. "When public key cryptography is broken, users could be losing their funds and the whole system will break."

Quantum computers get their power by manipulating data stored on qubits, elements like charged atoms that are subject to the peculiar physics governing the ultra-small. To crack encryption, quantum computers will need to harness thousands of qubits, vastly more than the dozens corralled by today's machines. The machines will also need persistent qubits that can perform calculations much longer than the fleeting moments possible right now.

But makers of quantum computers are working hard to address those shortcomings. They're stuffing ever more qubits into machines and working on quantum error correction methods to help qubits perform more-sophisticated and longer calculations.

"We expect that within a few years, sufficiently powerful computers will be available" for cracking blockchains open, said Nir Minerbi, CEO of quantum software maker Classiq Technologies.

Fixing cryptocurrencies' quantum computing problem

The good news for cryptocurrency fans is the quantum computing problem can be fixed by adopting the same post-quantum cryptography technology that the computing industry already has begun developing. The US government's National Institute of Standards and Technology (NIST), trying to get ahead of the problem, is several years into a careful process to find quantum-proof cryptography algorithms with involvement from researchers around the globe.

Indeed, several cryptocurrency and blockchain efforts are actively working on quantum resistant software:

- The Ethereum project, which created the biggest cryptocurrency after Bitcoin in terms of total value, has begun charting a post-quantum course. Justin Drake, a researcher at the Ethereum Foundation, detailed quantum resistance ideas in Ethereum 3.0 at the StarkWare conference in 2019. That's likely a long ways off, though: Ethereum's current transition to Ethereum 2.0 is taking years.

- Some people are building new cryptocurrency and blockchain technology designed for the quantum computing era. That includes Quantum Resistant Ledger and Bitcoin Post Quantum, which despite the name is unrelated to the original Bitcoin cryptocurrency. These efforts employ post-quantum algorithms to protect against future quantum cracking.

- Cambridge Quantum Computing, a startup merging with quantum computer maker Honeywell, is working on quantum security technology that "can be applied to any blockchain network." It aims to secure both the communications among computers storing blockchain data and the signatures used to encrypt and sign blockchain data.

- The Hyperledger Foundation, an open-source software project geared for business uses of blockchain, has begun working on post-quantum cryptography through its Ursa effort, says Daniela Barbosa, Hyperledger's executive director. Ursa is a library of cryptography software Hyperledger projects can use.

A problem with the post-quantum cryptography algorithms under consideration so far, though, is that they generally need longer numeric encryption keys and longer processing times, says Peter Chapman, CEO of quantum computer maker IonQ. That could substantially increase the amount of computing horsepower needed to house blockchains.

The problem with decentralized governance

Many cryptocurrencies, like Bitcoin, are decentralized by design, overseen in effect by anyone who participates in each cryptocurrency network. To update a cryptocurrency's inner workings, people trying to upgrade a cryptocurrency must convince more than half of participants to "fork" the cryptocurrency into a new version.

The real quantum test for cryptocurrencies will be governance structures, not technologies, says Hunter Jensen, chief technology officer of Permission.io, a company using cryptocurrency for a targeted advertising system.

Such governance could reward cryptocurrencies that have stronger central powers, such as Dash with its masternodes or even "govcoins" issued by central banks, that can in principle move more swiftly to adopt post-quantum protection. But it presents a conundrum in the crypto community, which often rejects the idea of authority.

"It will be the truly decentralized currencies which will get hit if their communities are too slow and disorganized to act," said Andersen Cheng, chief executive at Post Quantum, a London based company that sells post-quantum encryption technology.

Other quantum problems with cryptocurrencies

Another risk is that blockchains rely on a digital fingerprinting technology called hashing that quantum computers could disrupt. That's likely to be fixable with more-modest technology updates, though.

The cryptocurrency wallets people use to keep track of their digital assets could also be vulnerable to quantum computing. These wallets store private keys people need to access their assets recorded on the blockchain. A successful attack could empty a wallet.

"How do you force users to upgrade keys? That answer is not so straightforward and likely the most dangerous part," said Joe Genereux, senior cryptography and security engineer at browser maker Brave, which uses its own Basic Attention Token (BAT) cryptocurrency for an ad system that pays users. "I think cryptocurrencies that have better governance or post-quantum designs baked in early can get around this issue better."

Ultimately, though, cryptocurrency's organic, self-directed development suggests people will update the digital asset technology to surmount quantum computing's challenges, says David Sacco, who teaches at the University of New Haven.

"The beauty of the ecosystem," he said, "is that anyone can do it if they understand the technology."

25.IBM's Quantum Computer Tasked with Tackling Cancer Research in Europe

by Matt Swayne
https://thequantumdaily.com/2021/11/12/ibms-quantum-computer-tasked-with-tackling-cancer-research-in-europe/

IBM's quantum computer — the Q System 1 — is practically just out of the wrapper, but, according to Nature Biotechnology, it's already getting an important first mission: helping cancer researchers in Europe,

The device, billed as one of Europe's most powerful commercial quantum computers, is located at IBM's German headquarters in Ehningen, near Stuttgart and jointly operated by IBM and the Fraunhofer Society, Germany's multidisciplinary applied research organization.

The Fraunhofer Society will allow researchers to use the The 27-qubit quantum computer to test ideas for practical applications of quantum computers.

Biomedicine makes a natural fit for quantum computing because of the computationally intense and complex questions faced by researchers in the field.

The Fraunhofer Society hopes cancer researchers, among others, will use the device to explore research questions in oncology.

It's a big — and uncertain — first step.

"It's uncharted territory," oncologist Niels Halama of the DKFZ, Germany's national cancer center in Heidelberg, told Nature Biotechnology.

Halama is working with a team of physicists and computer scientists to develop and test algorithms that might help stratify cancer patients. The team will select small subgroups for specific therapies from heterogeneous data sets.
This is the beginning of precision medicine, something that classical computing struggles to accomplish. Classicomputing lacks the power to find small groups in the large and complex oncology data sets. The task, which can take weeks to accomplish on a regular device, isn't practical for doctors in a clinical setting and would be cost prohibitive, the journal states.

With the end of Moore's Law potentially nearing, these limits may be intractable.

While quantum faces its own challenges, researchers want to explore whether quantum, which theoretically could be speedier and more robust than classic, can deliver some of these solutions that precision medicine needs.

The researchers understand that noise — the ability of the environment to affect the calculations of extremely sensitive quantum devices — is the most significant challenge of quantum precision medicine.

"There is no guarantee that the quantum system will deliver the solutions we want," he tells Nature Biotechnology. "But there are indications that merit follow-up."

Hamala will use two different approaches. The team will create machine learning algorithms for quantum processing that might require smaller training datasets than conventional computing. It's an approach taken for human tumor data from the Cancer Genome Atlas. The other approach will use algorithms based on different mathematics—topological algebra, which quantum computing handles well—to sift through data for interesting patterns.

There's no reason that quantum computing would be restricted to just oncology. The devices may be vital to research in computational chemistry and biomedicine, and, in fact, across the life sciences.

Computational biologist Charlotte Deane, University of Oxford, told the journal she is taking this approach in her work on protein folding.

"It will speed up a limited number of tasks for us, and we need to correctly identify those tasks now," Deane said.

Deane is optimistic about quantum's potential.

"Quantum computing will become a tool of the trade for someone like me," Deane told the journal.

All research projects and user data remain in Germany, and the IBM Q System One operates in accordance with Germany's strict data-protection law, according to the journal.

The Q System 1 was just installed over the summer.

26.CINECA and AWS bring new quantum computing capabilities to the Italian research community

by Dr. Fabio Baruffa and Tyler Takeshita

https://aws.amazon.com/blogs/quantum-computing/cineca-and-aws-bring-new-quantum-computing-capabilities-to-the-italian-research-community/

CINECA and AWS are collaborating on a series of quantum computing research initiatives to help to accelerate the next generation of computational capabilities and enable new research in Italy.

CINECA is a consortium made up of 70 Italian universities and four national research institutes to form the leading high-performance computing (HPC) research center in Italy. CINECA operates one of the world's largest computing centers which supports cutting edge research by providing access to state-of-the-art HPC systems. One of their systems, Marconi-100, is ranked 14th in the TOP500 list of the most powerful supercomputer in the world.

To broaden CINECA's computational portfolio beyond classical computing, AWS and Cineca have launched a new collaboration to advance quantum computing research and education across Europe. CINECA has formed a steering committee of quantum computing experts drawn from the CINECA consortium to represent the voice of the quantum computing research community in Italy. This committee will help identify and shape cutting-edge quantum computing research projects that can leverage quantum computing services provided by AWS. AWS plans to support qualifying projects identified by CINECA via AWS Cloud Credits for Research, a program aimed to provide AWS credits to researchers across a range of disciplines.

To promote quantum skills in this interdisciplinary field, CINECA and AWS will host a series of workshops to deepen the quantum expertise of the HPC research community. CINECA-affiliated academics and developers from different scientific fields will have the opportunity to design and run quantum computational experiments on the cloud using Amazon Braket, the AWS quantum computing service. Amazon Braket provides on-demand access to different quantum computing technologies, circuit simulators, and a flexible development environment.

The first workshop, planned for November 24th, 2021, will be a Practical Quantum Computing School, an online course dedicated to the use of quantum computers in the cloud. This is a unique opportunity for students and researchers to gain hands-on experience in using quantum computers, while learning from leading experts in the field.

This collaboration with CINECA is a continuation of AWS's support of directed and independent research in quantum computing around the globe. If you are planning research in quantum computing, give Amazon Braket a try, or contact us via email, your AWS account manager or the AWS Cloud Credit for Research program.

27.In a quantum future, our economy needs to be protected. A cyber security expert explains why

by Abhinav Chugh

https://www.weforum.org/agenda/2021/11/in-a-quantum-future-our-economy-needs-to-be-protected-a-cybersecurity-expert-explains-why/

The privacy of online communication is currently protected by cryptography, which shields information as it travels around the internet. It secures everything from making online purchases to accessing work email remotely. With capabilities of quantum computing growing rapidly, industry experts reckon that it will take at least another 10 years before quantum computers with very large numbers of qubits are available.

Quantum computers could run algorithms that could break the public key encryption we use today. Researchers are performing intensive research to review, select and improve several dozen different algorithms to replace the current ones to prevent this.

The technology is still at an early stage and will take several decades before it reaches full fruition, which allows us a brief window to develop the current digital and IT infrastructure to be prepared for a quantum future.

We discussed why and how the current cyber landscape could develop and prioritise certain areas to avoid the potential harms and risks from developments in quantum computing with Jaya Baloo, Chief Information Security Officer at Avast.

Jaya has been working in the field of information security, with a focus on secure network architecture, for over 20 years and sits on the advisory boards of the Netherland's National Cyber Security Centre, PQCrypto and EU Quantum Flagship's Strategic Advisory Board. She is currently a member of the World Economic Forum's Global Future Council on Quantum Computing.

For many years, the quantum threat to cryptography was considered theoretical. However, with recent advances in building a physical quantum computer, Jaya believes we are not far from our currently used cryptographic algorithms breaking down.

What drew you towards developing your expertise in cyber security and becoming a leader in this domain?

I think I've always been curious about security. When I was a child, I was fascinated by phone phreaking and my interest developed in earnest when I was working as a network engineer at KPN. The fact is, once you get started in cyber security, it's hard to remain on the sidelines and instead you're very quickly drawn to taking a position because there are so many foundational dilemmas that we deal with just in a day's work. Global issues influence security teams at an incredibly operational level and include everything from the impact of geopolitics on supply chain security to policies on cryptography as well as the use of certain tooling to assess the security posture of networks.

What is most misunderstood about your work? What do you wish people knew?

The thing that is most misunderstood about working in cyber security is how it often becomes visually characterized by Hollywood. It is often depicted as incredibly fast paced and exciting, as a sort of cat and mouse game between hardened defenders and hooded attackers. Unfortunately, the truth is a lot more about doing the regular, diligent, routine, and day-to-day incremental efforts to prevent an attack or to analyze and respond to one when it does happen. In reality, it's still about a lot of dedicated people staring at their screens with very few car chases in between.

I wish people understood better just how fragile our cyber security position is and just how much effort we need to put in to improving the basics now to be prepared for the future. We still rely on foundational protocols that were developed in the 1970s and haven't changed a lot since then for our primary transmission communications layer. We have lots of new tools developed with old classes of vulnerabilities in them. We still don't proactively test and change rapidly enough to evolve in line with the new threats that we're facing. Added to that is that there's an enormous interdependency from a critical infrastructure point of view because we rely on the same tools all over the world, so a single successful attack has a very large ripple effect.

In your opinion, what is the most critical cyber security challenge that leaders currently face?

Currently, I think the biggest challenge that leaders face is understanding that we have excluded the cost of cyber security in our existing IT infrastructure. The sunk cost of these old investments means that fixing or upgrading is not always an easy decision and organizations have extensive risk management tactics to explain rather than adhere to best practices. When this is already a challenge, thinking about additional safeguards for new technology often seem to be a nice to have rather than a need to have unless compelled by regulatory requirements. A good practice is to reserve about ten percent of IT budget for your non personnel spend for information security. If all parties started doing that, our innovation capacity would catch up on our legacy infrastructure. Then, we would slowly but assuredly be more secure.

Why do we need a tighter focus on encryption as a guarantee of privacy and online safety?

Cryptography is at the heart of our global internet economy from online banking to guarding intellectual property as well as the more foundational need to have secure and private communications between individuals. It guards human rights but also supports national security. Unfortunately, this does not mean that we have not had challenges to this capability as evinced by the cryptography wars of the 1990s. It always makes me think of a quote by Benjamin Franklin, that "those who would give up essential liberty for a little bit of temporary safety deserve neither liberty nor safety", which speaks to the tension between national surveillance capabilities versus individual privacy needs. We need good, strong, well tested cryptography without backdoors in order to protect a free and democratic society. There are alternatives available for law enforcement to conduct targeted investigations without jeopardizing the common security available to us all and our fundamental human rights.

How could developments in quantum computing disrupt this?

The promise of quantum computing is that very long held and difficult scientific problems will be solvable in a novel way. Our current cryptography is based on difficult math problems, such as integer factorization and discrete logs, which would take our current computers a very long time to solve. However, a quantum computer of sufficient scale can speed up the solving of these problems so significantly that it will effectively break our currently used cryptographic algorithms.

What actions are required to enable a secure and sustainable transition to the quantum economy?

First things first, we need to know where we use our current cryptography and for what purpose. Most organizations have no idea what their cryptographic resources are and how it enables daily operations. Once we've completed that inventory, we need to figure out how to transition to new post quantum algorithms which are a new set of algorithms that will still be resistant to a quantum computing attack, while potentially also looking for very specific opportunities to deploy something called quantum communications (secure communications links based on the principles of quantum mechanics). Looking through an organization's supply chain, there may be vendors that are working in this area and will afford easy transition opportunities to an organization. However, no matter what, they should be thinking about it and just understanding a vendor's maturity in this area is vital to enable a smooth transition.

What would be your advice to policymakers and other cyber security experts to achieve this?

Although it would be wonderful if everyone just voluntarily adopted best practices habitually, I fear we require some regulatory framework and national strategy to make sure that the most vulnerable and critical parts of our economy are quantum ready. My biggest concern is the time we have left to transition to a secure post quantum future. It's important to be able to embrace the benefits of quantum computing and quantum technologies to advance our society while managing any potential downsides from the weakening on cryptography. Since there is such a strong strategic and national security advantage in terms of surveillance capabilities, I fear that certain infrastructure and software will find its way onto the Wassenaar Arrangement on export controls for conventional arms and dual use goods and technologies.

I would urge policy makers to ensure that there are no export restrictions against export of quantum technologies which would only further deepen the digital divide. Due to our interconnected economies, we need democratization of technology and must ensure global participation to be collectively secure, a sort of digital version of herd immunity.

28.BMW Group and Amazon Web Services Select QCI's 'Qatalyst' as a Finalist in the Quantum Computing Challenge

by Matt Swayne

https://thequantuminsider.com/2021/11/10/bmw-group-and-amazon-web-services-select-qcis-qatalyst-as-a-finalist-in-the-quantum-computing-challenge/

Quantum Computing Inc., a leader in bridging the power of classical and quantum computing, announced that its Qatalyst ready-to-run quantum software was selected as one of three finalists for the second and final round of the BMW Group and Amazon Web Services (AWS) Quantum Computing Challenge for the Vehicle Sensor Placement use case.

The Quantum Computing Challenge invited the quantum community to apply innovations in quantum computing to real world problems in industrial applications. The use case problems presented in the challenge represent critical commercial applications that demonstrate the real-world value of quantum computing.

BMW stated that its goal with the challenge is to "tap into additional innovative power, inspire new thinking, and create opportunities for quantum builders to work with BMW on meaningful business problems."

The Vehicle Sensor Placement use case challenges participants to find optimal configurations of sensors for a given vehicle so that it can reliably detect obstacles in different driving scenarios – using quantum computing or nature-inspired optimization approaches. The number of sensors per car is expected to increase significantly as autonomous driving becomes more common. Vehicles need sensors to gather data from as large a portion of their surroundings as possible, but each sensor adds additional costs, so optimizing the sensor placement uses genetic algorithms. The goal of the challenge is to use quantum computing techniques to optimize the positions of sensors, enabling maximum coverage while keeping costs to a minimum.

"This Challenge is yet another step in showcasing quantum computing's potential for commercial applications and real-world business problem solving," said Bob Liscouski, CEO of QCI. "We are pleased that we have been selected to participate in the final level of competition, and our team will work hard to demonstrate the power of Qatalyst. Regardless of the final outcome, we believe that the applications for quantum computing will significantly increase over the coming years, and QCI is well positioned to be a key player."

29.Classical Computing Strikes Back; Simulation Advances from NVIDIA and China

https://quantumcomputingreport.com/classical-computing-strikes-back-simulation-advances-from-nvidia-and-china/

One thing not fully understood is that significant innovation is still occurring in classical computing and those trying to demonstrate a quantum advantage over a classical solution will find that the competitive bar is continually being raised. Some will say that classical computing is slowing down because Moore's Law improvements are becoming harder to come by, but that is too simplistic. There is still much classical computing innovation still occurring in new architectures, new algorithms, and development of quantum-inspired solutions. Two recent announcements from GPU manufacturer NVIDIA and a research group in China show some significant advances in the classical simulation of quantum algorithms that may make these approaches much more attractive for use in real world problems.

The first announcement has come from NVIDIA which announced a software product called cuQuantum earlier this year that was specifically designed to accelerate quantum simulations. This product contains two libraries. The first is called cuStateVec which allows for a state vector simulation that supports tens of qubits, depending upon how much memory is available. The second is called cuTensorNet which uses a tensor network simulation approach that can potentially simulate some algorithm that require thousands of qubits. The news this week is that cuStateVec has now progressed to a public beta status and the cuTensorNet is expected to reach this state in December. Previously, this software was still under development and internal testing at NVIDIA. In addition, cuStateVec has already been integrated into qsim, Google Quantum AI's state vector simulator and is slated to be integrated next month into Qiskit AER, a simulation framework from IBM.

To show the potential power of these simulators, NVIDIA used their cuTensorNet library with their Selene supercomputer that has 896 GPUs to solve a Maxcut problem with 3,375 vertices. This required simulation of a quantum circuit that had 1688 qubits, an 8 times improvement over previous attempts. For more about NVIDIA's activities in using GPUs for simulation of quantum algorithms, can you view our previous article from earlier this year when they first announced it and also their latest announcement that describes their public beta, partnerships with IBM, Google, IonQ, Pasqal and others and also their large MaxCut demonstration.

You may remember that when Google announced their "quantum supremacy" experiment (which they have since renamed to "beyond classical") they indicated that finding a classical solution to the problem would take the largest classical computer about 10,000 years compared with 200 seconds on their Sycamore processor. Very shortly after that, IBM posted a rebuttal and provided a paper analysis of a different simulation algorithm and felt that the classical simulation could be accomplished in about 2.5 days. Now a group from the Chinese Academy of Sciences and Peking University has implemented an approach that achieves this in 15 hours using a cluster of 512 GPUs. They used a tensor network approach to solve the uncorrelated sampling problem based on contractions of the three-dimensional tensor network. Furthermore, they indicated that the times an be further improved by either by using the cuQuantum libraries from NVIDIA or using a modern supercomputer that can provide exaflops performance. Overall, they estimated that the time to solution could be reduced to a few dozens of seconds which would be much faster than Google's result on Sycamore. So the quantum supremacy would not supreme anymore! For more information about this team's approach to speed up the simulation times, you can view an arXiv preprint that they recently posted here.

30.A New Scientific Milestone in the Advanced Quantum Testbed (AQT) at Berkeley Lab

by Kenna Castleberry
https://thequantuminsider.com/2021/11/09/a-new-scientific-milestone-in-the-advanced-quantum-testbed-aqt-at-berkeley-lab/

A team of physicists and engineers at Lawrence Berkeley National Laboratory (Berkeley Lab) successfully demonstrated the feasibility of low-cost and high-performance radio frequency modules for qubit controls at room temperature. They built a series of compact radio frequency (RF) modules that mix signals to improve the reliability of control systems for superconducting quantum processors. Their tests proved that using modular design methods reduces the cost and size of traditional RF control systems while still delivering superior or comparable performance levels to those commercially available.

Their research, featured as noteworthy in the Review of Scientific Instruments and selected as a Scilight by the American Institute of Physics, is open source and has been adopted by other quantum information science (QIS) groups. The team expects the RF modules' compact design is suitable for adaptation to the other qubit technologies as well. The research was conducted at the Advanced Quantum Testbed (AQT) at Berkeley Lab, a collaborative research program funded by the U.S. Department of Energy's Office of Science.

A Question of Scale

Despite significant advances in building processors with more qubits, which will ultimately be needed to demonstrate a quantum advantage over classical computers, quantum computers continue to be noisy and error-prone. Each additional qubit introduces new layers of complexity and possibilities for electrical failure, especially at room temperature. This growth in complexity and computing power requires a rethinking of certain core control elements.

Traditional RF control systems use analog circuits to control superconducting qubits, but they can become bulky and overwhelmingly complex, thus serving as a potential point of failure and increasing the costs for hardware control.

AQT researchers Gang Huang and Yilun Xu from Berkeley Lab's Accelerator Technology and Applied Physics Division (ATAP) demonstrated a new way to control qubits that is already enhancing other quantum computing projects at the testbed's user program. The team substituted the larger, more costly traditional RF control systems for one built at Berkeley Lab, which uses smaller interactive mixing modules.

A key aspect of this modular system is delivering high-resolution, low-noise RF signals needed to manipulate and measure the superconducting qubit at room temperature. To do so, it's important to shift the qubit manipulation and measurement signal frequency between the electronics baseband and the quantum system.

"The new module exhibits low-noise, high-reliability operation and is now becoming our laboratory standard for microwave frequency modulation/demodulation across many different experimental configurations in AQT," Huang explained.

Using the team's low-noise RF mixing module to shift the bandwidth with a limited intermediate frequency between the electronics baseband and the quantum system intrinsic band allows researchers to utilize less noisy converters for better performance and at a lower cost.

Huang and Xu said that while their system was designed for superconducting systems, it could be expanded to other quantum information science platforms. "In general, the architecture of RF mixing can be expanded to higher frequencies," they noted. "Therefore, if we replace some electronic components with appropriate frequency, this kind of compact design should be able to adapt to the other qubit platforms, i.e., semiconductor qubit systems."

Researchers also designed electromagnetic interference shielding to eliminate undesired perturbations, which reduce signal integrity and limit overall performance. This shielding aims to prevent the signal from leaking out and interfering with surrounding electronics – a common problem for quantum computers.

Open Source, Open Hardware

With the release of a control system that is open source, the team hopes that the broader community uses and contributes to the repository, improving the hardware. By replacing a few electronic components with appropriate frequency, this kind of compact design may adapt to a variety of quantum computing facilities.

"This is one of our first efforts to develop an open source control system for superconducting quantum processors," explained Huang. "We will continue to optimize the physical size and cost of the module and further integrate with our FPGA-based controller to improve the extensibility of the qubit control system."

Looking ahead, the researchers are already building on these efforts to create new possibilities in quantum computing and offer a new technology to control qubits.

"Such integration and optimization will help room-temperature-based control systems keep pace with advancements in the complexity of quantum processors," noted Xu.

31.NVIDIA, Google Quantum AI, IBM, Others Team Up to Speed Research in Quantum Computing

by Matt Swayne
https://thequantumdaily.com/2021/11/09/nvidia-google-quantum-ai-ibm-others-team-up-to-speed-research-in-quantum-computing/

NVIDIA joined Google Quantum AI, IBM and other members of the quantum ecosystem to help speed up quantum research, according to a blog post.

NVIDIA announced at GTC 2021 that the cuQuantum software development kit was used to speed up simulations of quantum computers on classical system.

The NVIDIA team writes: "Quantum computing offers the promise of solving previously unsolvable problems in fields like drug development, climate research, machine learning and finance. The potential is great, but so are the challenges. Today's quantum computers may be too small and error-prone to solve useful problems, and it's not yet clear which quantum algorithms will provide advantages over today's classical computers."

Using classical computers to test quantum algorithms would give scientists a head start in designing these complex algorithms and to make sure the ones with the highest likelihood of success are prioritized, the team added.

The company's cuStateVec is an accelerator for the state vector simulation method, an approach that tracks the system's full state in memory and can scale to tens of qubits. A second library cuTensorNet, an accelerator using the tensor network method and manage thousands of qubits, is expected in December.

CuStateVec is integrated into qsim, Google Quantum AI's state vector simulator that can be used through Cirq, an open-source framework for programming quantum computers. Users can download cuQuantum and start using it today wherever they use Cirq, according to the post.

"Quantum computing promises to solve tough challenges in computing that are beyond the reach of traditional systems," said Catherine Vollgraff Heidweiller at Google Quantum AI. "This high-performance simulation stack will accelerate the work of researchers around the world who are developing algorithms and applications for quantum computers."

The company said that Oak Ridge, Argonne, Lawrence Berkeley National Laboratory and Pacific Northwest National Laboratory, university research groups at Caltech, Oxford and MIT, and companies including IonQ are integrating cuQuantum into their workflows.

Pasqal, a Paris-based quantum computing startup, purchased an NVIDIA DGX POD to perform massive simulations with cuQuantum with plans to apply it to accelerating work in areas such as drug design and smart mobility.

"The ability to perform powerful, large-scale simulations of quantum systems is vital to our work," said Loic Henriet, CTO at Pasqal. "The combination of cuQuantum software with DGX A100 hardware will dramatically accelerate our progress."

The first library from cuQuantum is in public beta, available to download.

32.New South Wales Government Envisions Quantum Computers Will One Day Manage its Transportation Network

by Matt Swayne

https://thequantumdaily.com/2021/11/08/new-south-wales-government-envisions-quantum-computers-will-one-day-manage-its-transportation-network/

The government of New South Wales will investigate the use of quantum computers to run its transportation network, Australian media are reporting.

The government will establish a center aimed at studying how quantum computers can be used in transportation, said Rob Stokes, NSW Transport Minister. The Centre of Quantum Technology will be built in Sydney's Tech Central and be administered by an advisory panel which includes NSW quantum pioneer and professor Michelle Simmons.

"The recovery from the pandemic makes it even more important because it's harder to predict," Stokes told the media. "Quantum computing can actually help us to deploy resources far more accurately, and we genuinely don't know what the long-term impacts of the pandemic are going to be on travel patterns and on travel preferences."

One of the hopes is that quantum computing can organize transportation more effectively reducing delays. Stokes added that he believes quantum may lead to a "self-healing" network that could interact with self-driving cars, artificial intelligence and smart sensors.

"While this might sound like the stuff of science fiction, Transport for NSW is making quantum computing a reality. It has the potential to solve problems on the network in real time by instantly recalculating timetables and routes," Stokes said.

Simmons said the use of quantum technology may be transformative for transportation — and beyond.

"It's a very powerful, transformational technology. It allows us to solve problems in real time that would otherwise take thousands of years," Simmons said in The Age. "Anyone who travels, whether it's by car, train, plane, you always want to minimise your time waiting around. You want things to be efficient. Some of the problems are so complex that classical computers can't solve them in a timeframe that's real for them."

Michael Biercuk, Sydney University Professor and Q-CTRL founder, described how quantum computing works and how it relates to transportation problems. (Learn more about Q-CTRL at The Quantum Insider.)

"We have the ability to put information into individual atoms, or individual circuits of special materials called superconductors, and when we do that we have a way to represent all the different ways that parts of the transport network are connected together," he said.

New South Wales in the southeastern tip of Australia and includes major transportation hubs, such as Sydney, Australia, the country's second largest city.

33.NSA Announces New Partnership with National Cryptologic Foundation

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2834755/nsa-announces-new-partnership-with-national-cryptologic-foundation/

In concert with remarks by General Paul M. Nakasone, Commander, U.S. Cyber Command, Director NSA/Chief, CSS, during the Aspen Security Forum, the National Security Agency (NSA) today announces a new partnership with the National Cryptologic Foundation.

The Agency will work with the Foundation to grow cybersecurity strength across the nation, focusing on cybersecurity education and building pipelines for cybersecurity jobs.

"Recruiting and retaining next generation talent are among our top priorities at the NSA," said GEN Nakasone. "Relationships to enhance our hiring efforts are fundamental to our ability to consistently provide world class foreign intelligence and cybersecurity expertise."

The partnership will include efforts to promote deeper understanding of past cryptologic successes pivotal to U.S. and allied democracies, support public/private collaboration to address emergent cybersecurity challenges, and enhance relationships with academia to develop and attract future cryptologists and cybersecurity professionals.

The National Cryptologic Foundation (NCF) is a cybersecurity-focused organization that serves as a platform for public/private dialog on cybersecurity and a provider of resources for nation-wide cyber education to grow cyber talent. The National Cryptologic Foundation was founded in 1996 as a 501 c(3) not for profit with a mission to "influence the cryptologic future by sharing our educational resources, stimulating new knowledge and commemorating our heritage." The Foundation's three primary objectives are to: Educate the public, Stimulate public engagement, and Commemorate and celebrate all who have "served in silence" in service to our nation.

34.Practical distributed quantum information processing with LOCCNet

by Xuanqiang Zhao, Benchi Zhao, Zihe Wang, Zhixin Song and Xin Wang

https://www.nature.com/articles/s41534-021-00496-x

Distributed quantum information processing is essential for building quantum networks and enabling more extensive quantum computations. In this regime, several spatially separated parties share a multipartite quantum system, and the most natural set of operations is Local Operations and Classical Communication (LOCC). As a pivotal part in quantum information theory and practice, LOCC has led to many vital protocols such as quantum teleportation. However, designing practical LOCC protocols is challenging due to LOCC's intractable structure and limitations set by near-term quantum devices. Here we introduce LOCCNet, a machine learning framework facilitating protocol design and optimization for distributed quantum information processing tasks. As applications, we explore various quantum information tasks such as entanglement distillation, quantum state discrimination, and quantum channel simulation. We discover protocols with evident improvements, in particular, for entanglement distillation with quantum states of interest in quantum information. Our approach opens up new opportunities for exploring entanglement and its applications with machine learning, which will potentially sharpen our understanding of the power and limitations of LOCC. An implementation of LOCCNet is available in Paddle Quantum, a quantum machine learning Python package based on PaddlePaddle deep learning platform.

35.Securing data transfers with relativity

by Nicolas Brunner and Hugo Zbinden

https://www.unige.ch/communication/communiques/en/2021/securiser-les-transferts-de-donnees-grace-a-la-relativite/

The volume of data transferred is constantly increasing, but the absolute security of these exchanges cannot be guaranteed, as shown by cases of hacking frequently reported in the news. To counter hacking, a team from the University of Geneva (UNIGE), Switzerland, has developed a new system based on the concept of “zero-knowledge proofs”, the security of which is based on the physical principle of relativity: information cannot travel faster than the speed of light. Thus, one of the fundamental principles of modern physics allows for secure data transfer. This system allows users to identify themselves in complete confidentiality without disclosing any personal information, promising applications in the field of cryptocurrencies and blockchain. These results can be read in the journal Nature.

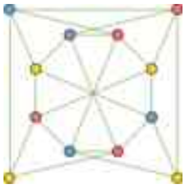
When a person – the so called ‘prover– ’ wants to confirm their identity, for example when they want to withdraw money from an ATM, they must provide their personal data to the verifier, in our example the bank, which processes this information (e.g. the identification number and the pin code). As long as only the prover and the verifier know this data, confidentiality is guaranteed. If others get hold of this information, for example by hacking into the bank’s server, security is compromised.

Zero-knowledge proof as a solution

To counter this problem, the prover should ideally be able to confirm their identity, without revealing any information at all about their personal data. But is this even possible? Surprisingly the answer is yes, via the concept of a zero-knowledge proof. “Imagine I want to prove a mathematical theorem to a colleague. If I show them the steps of the proof, they will be convinced, but then have access to all the information and could easily reproduce the proof”, explains Nicolas Brunner, a professor in the Department of Applied Physics at the UNIGE Faculty of Science. “On the contrary, with a zero-knowledge proof, I will be able to convince them that I know the proof, without giving away any information about it, thus preventing any possible data recovery.”

The principle of zero-knowledge proof, invented in the mid-1980s, has been put into practice in recent years, notably for cryptocurrencies. However, these implementations suffer from a weakness, as they are based on a mathematical assumption (that a specific encoding function is difficult to decode). If this assumption is disproved – which cannot be ruled out today – security is compromised because the data would become accessible. Today, the Geneva team is demonstrating a radically different system in practice: a relativistic zero-knowledge proof. Security is based here on a physics concept, the principle of relativity, rather than on a mathematical hypothesis. The principle of relativity – that information does not travel faster than light – is a pillar of modern physics, unlikely to be ever challenged. The Geneva researchers’ protocol therefore offers perfect security and is guaranteed over the long term.

Dual verification based on a three-colorability problem



Implementing a relativistic zero-knowledge proof involves two distant verifier/prover pairs and a challenging mathematical problem. “We use a three-colorability problem. This type of problem consists of a graph made up of a set of nodes connected or not by links”, explains Hugo Zbinden, professor in the Department of Applied Physics at the UNIGE. Each node is given one out of three possible colours – green, blue or red – and two nodes that are linked together must be of different colours. These three-colouring problems, here featuring 5,000 nodes and 10,000 links, are in practice impossible to solve, as all possibilities must be tried. So why do we need two pairs of checker/prover?

“To confirm their identity, the provers will no longer have to provide a code, but demonstrate to the verifier that they know a way to three-colour a certain graph”, continues Nicolas Brunner. To be sure, the verifiers will randomly choose a large number of pairs of nodes on the graph connected by a link, then ask their respective prover what colour the node is. Since this verification is done almost simultaneously, the provers cannot communicate with each other during the test, and therefore cannot cheat. Thus, if the two colours announced are always different, the verifiers are convinced of the identity of the provers, because they actually know a three-colouring of this graph. “It’s like when the police interrogates two criminals at the same time in separate offices: it’s a matter of checking that their answers match, without allowing them to communicate with each other”, says Hugo Zbinden. In this case, the questions are almost simultaneous, so the provers cannot communicate with each other, as this information would have to travel faster than light, which is of course impossible. Finally, to prevent the verifiers from reproducing the graph, the two provers constantly change the colour code in a correlated manner: what was green becomes blue, blue becomes red, etc. “In this way, the proof is made and verified, without revealing any information about it”, says the Geneva-based physicist.

A reliable and ultra-fast system

In practice, this verification is carried out more than three million times, all in less than three seconds. “The idea would be to assign a graph to each person or client”, continues Nicolas Brunner. In the Geneva researchers’ experiment, the two prover/verifier pairs are 60 metres apart, to ensure that they cannot communicate. “But this system can already be used, for example, between two branches of a bank and does not require complex or expensive technology”, he says. However, the research team believes that in the very near future this distance can be reduced to one metre. Whenever a data transfer has to be made, this relativistic zero-knowledge proof system would guarantee absolute security of data processing and could not be hacked. “In a few seconds, we would guarantee absolute confidentiality”, concludes Hugo Zbinden.

36.Qrypt releases two solutions to ensure quantum-secure encryption for businesses

https://www.helpnetsecurity.com/2021/11/03/qrypt-quantum-encryption/

Qrypt launched two new solutions: the Cloud Enterprise Portal, and Digital Quantum Key Distribution (Digital QKD). This expands on Qrypt's Entropy-as-a-Service (EaaS) portfolio which provides high-quality quantum random numbers and the tools to ensure Everlasting Security. Enterprises can now integrate quantum encryption into their software services with tools that are fast, easy to use, highly scalable, and don't require expensive infrastructure.

"Our Digital QKD and Cloud Enterprise Portal solutions are a big step toward the founding goal of Qrypt which is to help organizations protect their data and their consumers' privacy," said Kevin Chalker, Qrypt's CEO, and founder. "As current data encryption practices are quickly becoming obsolete, the first businesses to integrate quantum encryption will find themselves at a competitive security advantage compared to their rivals."

In a world where the threat of system vulnerabilities and data breaches is at a near-constant, businesses need to protect themselves and their customers' data. All enterprises have some type of high-value data, and the security methods employed are often inadequate against determined attackers. For example, a bad actor could guess seeds based on previously unobserved patterns in what was thought to be a random source.

In addition, a "harvest now, decrypt later" attack could occur, where encrypted data is stolen in anticipation of quantum computers being able to decrypt it in the future. The effort to secure data can only be successful with high-quality random numbers, based on quantum effects, as they do not have an underlying pattern to exploit. An encryption system is also needed, that uses keys based on high-quality random.

Qrypt's technology is perfect for any business that needs to protect and secure vital data, either by integrating a trusted QRNG into an existing encryption infrastructure or to implement a full cryptographic solution. The risk of a data breach is completely nullified as stolen data can never be forcibly decrypted – even by quantum computers. Qrypt's solutions can be integrated into messaging and email platforms, file sharing services, and even network infrastructure for ISPs and financial institutions.

Qrypt's Digital QKD enables quantum-secure encryption keys to be generated and distributed to any connected endpoint or device – providing businesses quantum-secure encryption even on the public internet. Through creating an authenticated network of QRNGs in the cloud, quantum secure encryption is made massively scalable and easier for businesses to deploy. It avoids the costly infrastructure requirements and limitations of on-premise QKD appliances, and instead shifts key creation to the cloud on the Qrypt Cloud Enterprise Portal.

"Sensitive data needs a high-security crypto environment where it's done the right way," said Charles White, CTO of Fornetix. "Qrypt has the right approach with their innovative cloud-based quantum entropy and sophisticated digital QKD. Their one-time pad technology allows organizations that need next-level data protection to stay ahead of the curve."

The Cloud Enterprise Portal allows enterprises to employ quantum-secure random numbers into any in-house cryptographic key generation with improved speed and bandwidth. Whether leveraging classical or PQC, companies will be able to implement Qrypt's technology to deploy vastly larger key sizes – up to full one-time pad systems – for their business applications. Additionally, this offering includes a full suite of enterprise features, like multi-tenancy, access control capabilities, and new security options.

“These solutions will empower DevOps and SecOps teams at any enterprise, including financial institutions, healthcare organizations, and government agencies with the essential tools to protect themselves from the security threats of the quantum age,” said Denis Mandich, Qrypt CTO, and co-founder. “Qrypt’s digital QRNG technology is incredibly sophisticated due to years of intensive research and close partnerships with leading laboratories for quantum entropy sources.”

Unlike some competing solutions, Qrypt’s QRNG technology is powered by true random from measuring quantum effects. Thanks to exclusive partnerships with national and international labs including Oak Ridge, Pacific Northwest, Los Alamos, and EPFL for quantum entropy sources, Qrypt is the first EaaS provider to leverage multiple quantum sources. This allows Qrypt to deliver the highest quality of randomness for its security solutions – ensuring quantum-secure encryption for businesses.

37.The US is worried that hackers are stealing data today so quantum computers can crack it in a decade

by Patrick Howell O'Neill

https://www-technologyreview-com.cdn.ampproject.org/c/s/www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/amp/

While they wrestle with the immediate danger posed by hackers today, US government officials are preparing for another, longer-term threat: attackers who are collecting sensitive, encrypted data now in the hope that they’ll be able to unlock it at some point in the future.

The threat comes from quantum computers, which work very differently from the classical computers we use today. Instead of the traditional bits made of 1s and 0s, they use quantum bits that can represent different values at the same time. The complexity of quantum computers could make them much faster at certain tasks, allowing them to solve problems that remain practically impossible for modern machines—including breaking many of the encryption algorithms currently used to protect sensitive data such as personal, trade, and state secrets.

While quantum computers are still in their infancy, incredibly expensive and fraught with problems, officials say efforts to protect the country from this long-term danger need to begin right now.

“The threat of a nation-state adversary getting a large quantum computer and being able to access your information is real,” says Dustin Moody, a mathematician at the National Institute of Standards and Technology (NIST). “The threat is that they copy down your encrypted data and hold on to it until they have a quantum computer.”

“Adversaries and nation states are likely doing it,” he says. “It’s a very real threat that governments are aware of. They’re taking it seriously and they’re preparing for it. That’s what our project is doing.”

Faced with this “harvest now and decrypt later” strategy, officials are trying to develop and deploy new encryption algorithms to protect secrets against an emerging class of powerful machines. That includes the Department of

Homeland Security, which says it is leading a long and difficult transition to what is known as post-quantum cryptography.

“We don’t want to end up in a situation where we wake up one morning and there’s been a technological breakthrough, and then we have to do the work of three or four years within a few months—with all the additional risks associated with that,” says Tim Maurer, who advises the secretary of homeland security on cybersecurity and emerging technology.

DHS recently released a road map for the transition, beginning with a call to catalogue the most sensitive data, both inside the government and in the business world. Maurer says this is a vital first step “to see which sectors are already doing that, and which need assistance or awareness to make sure they take action now.”

Preparing in advance

Experts say it could still be a decade or more before quantum computers are able to accomplish anything useful, but with money pouring into the field in both China and the US, the race is on to make it happen—and to design better protections against quantum attacks.

The US, through NIST, has been holding a contest since 2016 that aims to produce the first quantum-computer-proof algorithms by 2024, according to Moody, who leads NIST’s project on post-quantum cryptography.

38.World-First Quantum Research Breakthrough Allows for Full Spin Qubit Control

by Francisco Piers
https://www.tomshardware.com/news/quantum-computing-breakthrough-qubit-control

A research team with Denmark's University of Copenhagen has designed the world's first quantum computing system that allows for simultaneous operation of all its qubits without threatening quantum coherence. The research is being hailed as a breakthrough, clearing one of the remaining key obstacles for quantum scaling and its eventual mainstream deployment.

As quantum computing is still in its nascent stages, there are a number of technologies — and qubit types — concurrently being explored. The Danish team achieved its breakthrough in one particular type of qubit, spin qubits. You may remember these from our recent article on quantum benchmarks, where a company that is also employing the spin qubit approach, IonQ, achieved remarkable results compared to other systems.

"To get more powerful quantum processors, we have to not only increase the number of qubits, but also the number of simultaneous operations, which is exactly what we did," states Professor Kuemmeth, who directed the research.

As it stands, two important elements on the road to quantum computing are scaling, as in, adding more and more qubits (think computer cores) so that the system's processing capabilities increase; and coherence, as in, how stable the system is during workload processing, and how accurate its results are. With quantum scaling well on its way already, this research focuses on the coherence part of the equation. The scaling part of the problem has already seen incredible progress, but the same hasn't been true about the coherence part of the equation — until now.

"Now that we have some pretty good qubits, the name of the game is connecting them in circuits which can operate numerous qubits, while also being complex enough to be able to correct quantum calculation errors," says Anasua Chatterjee, a member of the research team. "Thus far, research in spin qubits has gotten to the point where circuits contain arrays of 2x2 or 3x3 qubits. The problem is that their qubits are only dealt with one at a time."

Think of it this way: you can't read the content of a letter until you actually manipulate the envelope they're in, opening it to scan what's inside. However, much in the same way that you change the state of the envelope in reaching the letter proper, qubits are changed when you try to read them. With quantum physics, manipulating a single qubit has up to now resulted in (essentially) catastrophic decoherence of the surrounding system. Basically, the results stop being accurate. This research now proves there is a way to operate and measure the entire qubit subsystem without that fall to chaos.

Chaterjee states, "The new and truly significant thing about our chip is that we can simultaneously operate and measure all qubits. This has never been demonstrated before with spin qubits — nor with many other types of qubits."

Of course, the breakthrough won't be able to stand on its own; research work is never done. As such, the researchers have identified the most pressing limitations on their approach. While the control mechanism employed by the scientists has been proven to maintain quantum coherence, its current design requires sustained, manual tuning of the 48 control electrodes that actually make the system work. The team is now looking to AI control systems that could automatically keep the system tuned with no human intervention. Perhaps this breakthrough will bring renewed focus on spin qubits as the fastest way to achieve a scalable, coherent, and efficient quantum computer. Time will tell.

39.All-in-one quantum key distribution system makes its debut

by Karmela Padavic-Callaghan

https://physicsworld.com/a/all-in-one-quantum-key-distribution-system-makes-its-debut/

A future in which quantum computers are commonplace might seem like an optimistic fantasy, but it could also involve hackers using those computers to steal important information. To thwart would-be bad actors, researchers developed a cryptographic protocol known as quantum key distribution (QKD) that uses the laws of quantum mechanics to enhance communication security. A team from Toshiba Europe Ltd has now combined a set of chips into compact modules order to build an entire standalone QKD system for the first time, miniaturizing and integrating key components and showing that the resulting system can transmit information autonomously, stably and securely for days, and over tens of kilometres.

One of the miniaturized components in the Toshiba team's system is a credit-card-sized transmitter chip that encodes quantum information into light. To do this, a laser produces a very faint pulse that contains, on average, one photon. Information is then "written" into this photon's precisely tuned quantum mechanical properties in a way that can be decoded by a receiver chip. Importantly, scientists designed the quantum decoding process to be sensitive to any potential eavesdroppers. In other words, had someone intercepted the communication between the two chips, the system would have recognized that "attack" every time.

The new system also includes two photon-based quantum random number generators (QRNGs). These devices govern how the transmitter chip prepares the photonic quantum bits, or qubits, that encode information, and the way the receiver decodes that information. By producing numbers that are so random that they are essentially impossible to guess, QRNGs provide another valuable contribution to the security of the new QKD system, explains Taofiq

Paraiso, a research scientist at Toshiba and the first author of a new paper in *Nature Photonics* that describes the company's system.

All-in-one package

According to Paraiso's colleague Thomas Roger, previous demonstrations of QKD systems often did not perform quantum random number generation in real time, or at the same time as they transmitted information. The Toshiba system, in contrast, combines multiple processes, including QRNG, into an all-in-one package that is smaller and more cost-effective than many of its predecessors. "This is the first time that the three chips – quantum transmitter, quantum receiver and QRNG – work together to distil a key from a QKD system," agrees Marco Lucamarini, a physicist at the University of York, UK, who was not involved with the experiment. Lucamarini also notes that the experimenters removed all the usual supporting lab equipment to test their system, leaving only the chips themselves and the fast electronics that connect them.

While photonic chips have been used in quantum information applications before, Paraiso says it was not previously clear that full system integration was possible. "We put a whole lot of effort into integrating all chips into one system and developing the electronics interface so that all the chips can talk to each other," he says, adding that the team designed its chips and electronics to be as simple as possible while minimizing the overall power consumption and bulkiness of the setup. Additionally, the designers placed all chips involved in security-critical quantum processes inside pluggable modules already used in conventional optical communications systems.

The importance of integration

The future of quantum communication networks will hinge on the practicality of such integration efforts, says Paolo Villoresi, director of the Padua Quantum Technologies Research Center at the University of Padua, Italy. He explains that researchers like himself and members of the Toshiba team are working to move quantum information systems out of the "unwieldy collections of discrete components" stage of their development by using photonic integration technology that has been shown to work well for standard optical communication networks. "Integrated photonics is sort of following the steps of integrated electronics," he says. He takes the comparison further: "Nowadays no one is considering going back to bulk transistors."

Lucamarini agrees, identifying integration as one that is most important issues for practical and commercial uses of QKD. "Scaling bulky QKD systems down to the size of a coin and integrating them in pluggable modules reduces size, energy consumption and cost, therefore bringing this technology much closer to the market," he says, adding that integrated photonic chips could be mass produced via methods that are already standard in the semiconductor industry.

Although the Toshiba system is still a prototype, members of the team are enthusiastic about the progress their interdisciplinary group of scientists – who specialize in areas ranging from optics to QRNG – has made. The new experiment showed that the system not only works alongside commercially available encryption systems, but can also operate for weeks or even months at a time without significant errors. In future, they hope to make it yet more compact and, eventually, integrate it into existing conventional communications networks. "There are some subtleties about classical communications networks so you can't just put in a QKD system and expect it to work across the whole network," Roger says. "We need to add infrastructure, but that's something that's happening." Villoresi concurs: "Integrated quantum photonics is a field that is currently very alive and vivid." The new experiment, he says, is an example of how a complete, integrated photon based QKD systems can work in the world outside the lab.

40.Quantum computers: Eight ways quantum computing is going to change the world

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/quantum-computers-eight-ways-quantum-computing-is-going-to-change-the-world/

The world's biggest companies are now launching quantum computing programs, and governments are pouring money into quantum research. For systems that have yet prove useful, quantum computers are certainly garnering lots of attention.

The reason is that quantum computers, although still far from having reached maturity, are expected to eventually usher in a whole new era of computing -- one in which the hardware is no longer a constraint when resolving complex problems, meaning that some calculations that would take years or even centuries for classical systems to complete could be achieved in minutes.

From simulating new and more efficient materials to predicting how the stock market will change with greater precision, the ramifications for businesses are potentially huge. Here are eight quantum use cases that leading organisations are exploring right now, which could radically change the game across entire industries.

(i) DISCOVERING NEW DRUGS
(ii) CREATING BETTER BATTERIES
(iii) PREDICTING THE WEATHER
(iv) PICKING STOCKS
(v) PROCESSING LANGUAGE

For decades, researchers have tried to teach classical computers how to associate meaning with words to try and make sense of entire sentences. This is a huge challenge given the nature of language, which functions as an interactive network: rather than being the 'sum' of the meaning of each individual word, a sentence often has to be interpreted as a whole. And that's before even trying to account for sarcasm, humour or connotation.

As a result, even state-of-the-art natural language processing (NLP) classical algorithms can still struggle to understand the meaning of basic sentences. But researchers are investigating whether quantum computers might be better suited to representing language as a network -- and, therefore, to processing it in a more intuitive way.

The field is known as quantum natural language processing (QNLP), and is a key focus of Cambridge Quantum Computing (CQC). The company has already experimentally shown that sentences can be parameterised on quantum circuits, where word meanings can be embedded according to the grammatical structure of the sentence. More recently, CQC released lambeq, a software toolkit for QNLP that can convert sentences into a quantum circuit.

(vi) HELPING TO SOLVE THE TRAVELLING SALESMAN PROBLEM

A salesman is given a list of cities they need to visit, as well as the distance between each city, and has to come up with the route that will save the most travel time and cost the least money. As simple as it sounds, the 'travelling salesman problem' is one that many companies are faced with when trying to optimise their supply chains or delivery routes.

With every new city that is added to the salesman list, the number of possible routes multiplies. And at the scale of a multinational corporation, which is likely to be dealing with hundreds of destinations, a few thousand fleets and strict deadlines, the problem becomes much too large for a classical computer to resolve in any reasonable time.

Energy giant ExxonMobil, for example, has been trying to optimise the daily routing of merchant ships crossing the oceans -- that is, more than 50,000 ships carrying up to 200,000 containers each, to move goods with a total value of $14 trillion.

Some classical algorithms exist already to tackle the challenge. But given the huge number of possible routes to explore, the models inevitably have to resort to simplifications and approximations. ExxonMobil, therefore, teamed up with IBM to find out if quantum algorithms could do a better job.

Quantum computers' ability to take on several calculations at once means that they could run through all of the different routes in tandem, allowing them to discover the most optimal solution much faster than a classical computer, which would have to evaluate each option sequentially.

ExxonMobil's results seem promising: simulations suggest that IBM's quantum algorithms could provide better results than classical algorithms once the hardware has improved.

(vii) REDUCING CONGESTION

(viii) PROTECTING SENSITIVE DATA

Modern cryptography relies on keys that are generated by algorithms to encode data, meaning that only parties granted access to the key have the means to decrypt the message. The risk, therefore, is two-fold: hackers can either intercept the cryptography key to decipher the data, or they can use powerful computers to try and predict the key that has been generated by the algorithm.

This is because classical security algorithms are deterministic: a given input will always produce the same output, which means that with the right amount of compute power, a hacker can predict the result.

This approach requires extremely powerful computers, and isn't considered a near-term risk for cryptography. But hardware is improving, and security researchers are increasingly warning that more secure cryptography keys will be needed at some point in the future.

One way to strengthen the keys, therefore, is to make them entirely random and illogical -- in other words, impossible to guess mathematically.

And as it turns out, randomness is a fundamental part of quantum behaviour: the particles that make up a quantum processor, for instance, behave in completely unpredictable ways. This behaviour can, therefore, be used to determine cryptography keys that are impossible to reverse-engineer, even with the most powerful supercomputer.

Random number generation is an application of quantum computing that is already nearing commercialisation. UK-based startup Nu Quantum, for example, is finalizing a system that can measure the behavior of quantum particles to generate streams of random numbers that can then be used to build stronger cryptography keys.

41.Chinese Scientists Create Quantum Processor 60,000 Times Faster Than Current Supercomputers

by Jack Dunhill

https://www.iflscience.com/technology/chinese-scientists-create-quantum-processor-60000-times-faster-than-current-supercomputers/

The race is on to develop a quantum computer that can outpace a conventional supercomputer, and researchers from around the world are full-steam ahead. If scaled to adequate sizes, quantum computers represent the largest leap forward in computing for decades, carrying the potential to leave our current machines in the dust, but significant hurdles still remain.

Now, a team of researchers from China have created a superconducting quantum processor with 66 functional qubits which, when faced with a complex sampling task, was able to blast past even the most powerful supercomputers and complete it in just a fraction of the time. What makes the research so impressive is how it demonstrates a huge leap towards quantum primacy, a milestone in which quantum computers complete a task that is infeasible for a conventional computer to complete.

The research is published in Physical Review Letters.

The team is led by Jian-Wei Pan at the University of Science and Technology of China, who have produced both this superconducting processor, and an alternative system that uses photonics, or light. To achieve quantum primacy, the team aimed to use ‘sampling problems’ as their computational task, which involve problems whose solutions are not just singular, but multiple random ‘samples’ along a probability distribution. With such vast potential outputs, it is possible to create a sampling problem that a conventional computer cannot feasibly tackle, but quantum computers can, and thus demonstrate quantum primacy.

To that end, Pan and colleagues must upscale quantum processors. Quantum computers use qubits to process data, and the creation of a viable quantum system requires quantum processors involving more qubits than currently possible. The largest quantum processors can currently process around 50 qubits, largely due to physical limitations on the chip. Pan’s new tunable superconducting processor, called Zuchongzhi, features 66 functional qubits.

When presented with an extremely complex sampling problem, estimated by the researchers to be 2-3 times more demanding than previous problems assigned to quantum processors, Zuchongzhi finished it in 1.2 hours. Pan and colleagues expect the same problem would require 8 years to be completed by the most powerful supercomputers.

In this case, the researchers only utilized 56 qubits for the sampling problem, which is 3 qubits more than a previous claim to primacy by Google. However, even such a small jump requires far more computational power to complete for a conventional computer, hopefully cementing their claim to primacy.

Every time researchers claim primacy, it is met with intense skepticism. Such skepticism involves the thought that the most ideal algorithms for the job are not used when conventional computers are pitted against the quantum options, but with such an increase over previous claims, Pan and colleagues hope to fully settle the debate that primacy has been achieved.

So, what does this all mean? Firstly, with regards to sampling problems, it appears quantum computers are finally significantly better than conventional options. That isn't to say they are practical just yet – far more innovation is required before quantum computers are used for actual tasks, and this will likely not occur too soon. However, there is a strong possibility that for some computational tasks, quantum processors might be the perfect solution, and could see use in niche scenarios in the future.