Crypto News

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

April 4, 2021

Contents

March 2021

31 Mar 2021

1 Detector-Integrated On-Chip QKD Receiver For GHz Clock Rates

by Karine

https://thequantumhubs.com/detector-integrated-on-chip-qkd-receiver-for-ghz-clock-rates/

Quantum Key Distribution (QKD) can greatly benefit from photonic integration, which enables implementing low-loss, alignment-free, and scalable photonic circuitry. At the same time, Superconducting Nanowire Single-Photon Detectors (SNSPD) are an ideal detector technology for QKD due to their high efficiency, low dark-count rate, and low jitter.

Researchers have developed a QKD receiver chip featuring the full photonic circuitry needed for different time-based protocols, including single-photon detectors.

By utilizing waveguide-integrated SNSPDs, they achieved low dead times together with low dark-count rates and demonstrate a QKD experiment at 2.6 GHz clock rate, yielding secret-key rates of 2.5 Mbit/s for low channel attenuations of 2.5 dB without detector saturation.

Due to the broadband 3D polymer couplers the receiver chip can be operated at a wide wavelength range in the telecom band, thus paving the way for highly parallelized wavelength-division multiplexing implementations.

2 New code breaking record for quantum-safe cryptography

by CWI

https://www.cwi.nl/news/2021/new-code-breaking-record-for-quantum-safe-cryptography

A team of cryptanalysts from Centrum Wiskunde & Informatica (CWI) has set a new code breaking record for an important computational problem: **the lattice shortest vector problem (SVP)**. Lattice SVP is a foundation for the security of next generation public-key cryptography, designed to be secure against quantum computers. Their result is a new frontier in the computational state-of-the-art of cryptographic techniques, making use of high-performance graphics cards. This research is aimed to provide crucial insights into secure parameter choices for next generation cryptography. The team's paper 'Advanced Lattice Sieving on GPUs, with Tensor Cores' was accepted this month for the Eurocrypt 2021 conference, which takes place in October.

Internet and computer security are founded on cryptographic standards, enabling HTTPS security, electronic banking, signing documents, and software standards. Public-key cryptography (PKC) is fundamental for these applications. The most common PKC systems are built on specific mathematical computational problems, called the integer factoring problem and the discrete log problem. As long as you make these problems too difficult to solve, these cryptographic systems are safe. But although these systems meet the security requirements of today, in theory they can be broken using a large-scale general quantum computer in the future.

Shortest Vector Problem

In order to provide security against quantum computers, cryptologists design the next generation of public-key cryptography based on other mathematical problems studied for decades. One of these alternatives are lattices: a grid of points in a multidimensional space. The security of lattice-based cryptography depends on the hardness of certain lattice problems, the most central one being finding the shortest vector in the lattice of large dimension. The difficulty of this problem can be vastly increased by using more and more dimensions, making it increasingly difficult to solve – and therefore break – by both classical and quantum computers.

Challenge

Researchers of CWI's Cryptology group have now solved the short vector problem for 180 dimensions in 52 days. The record was set as part of the Darmstadt Lattice Challenges, which was created to encourage cryptanalysis into lattice-based cryptography. The challenges consist of lattices of varying dimension and varying computational problems, including the most prominent: the shortest vector problem.

The team was composed of Leo Ducas, Marc Stevens and Wessel van Woerden, members of the CWI Cryptology group, headed by Prof. Ronald Cramer. The group investigates fundamental cryptographic questions from a broad scientific perspective, particularly from mathematics, computer science and physics.

Special machine

The team set the 52-day record using a special machine with 1.5 TB of RAM and four AI-capable graphics cards. The team has leveraged significant advances in cryptanalytic techniques as well as the exceptional computational power of the used graphic cards. Their NVIDIA RTX-2080 cards contain special high-performance tensor cores designed for AI and ray-tracing computations.

In comparison, the top-level record four years ago for a 150-dimensional lattice was achieved using several supercomputers taking more than a year. Since then, another approach called lattice sieving has taken the lead solving SVP up to dimension 155 in only weeks, where available resources limited immediate further progress. According to the researchers, with their new algorithmic improvements to sieving and using graphics cards, solving the 150-dimensional SVP takes only about one hour on their single machine and enables them to reach 180-dimensional SVP.

Why is this important and urgent

Lattice-based cryptography systems are considered a candidate for providing the first cryptographic standard to protect sensitive electronic data against the threat of quantum computers. To drive the development of the new standards, the US National Institute of Standards and Technology (NIST) is running a competition for new public-key cryptography standards secure against quantum computers. Among the seven schemes selected as finalists of the NIST competitions, five of them rely on lattices, including two designed in part at CWI.

Urgency

Even though sufficiently large quantum computers are unlikely to exist in the next decade or more, there is great urgency. It will take many years to actually deploy the upcoming standards. Meanwhile data protected by our current old cryptosystems can be eavesdropped and stored now to be broken later on.

Cryptographers crucially rely on large continuous cryptanalysis efforts, to expose weaknesses and deprecate weak standards. Another important goal is to validate the recommended key sizes and potentially increase them, similar to the RSA factoring efforts over the last decades in which CWI has also been involved.

This state-of-the-art cryptanalysis supports the proposed conservatively chosen key sizes to be secure. The computational cost grows exponentially, more doubling every four extra dimensions. Extrapolating suggests that breaking the NIST candidates – which would require solving SVP in dimensions greater than 400 – costs several billions of billions more computational effort. While this sounds astronomically infeasible, cryptographers usually keep sizable security margins in prediction of future progress on algorithms and hardware.

One question that might arise when the next record will be set. The CWI researchers estimate that they've essentially reached what is feasible with their algorithm on this high-end machine, even if they would let it run longer. Indeed, the required memory grows with each added dimension, and the SVP challenge of 180 dimensions already consumed the 1.5 Terabytes of RAM in their machine. Going further will require significantly more resources: clusters of several machines and/or hard drive storage. This raises further challenges to make effective use of such resources given the limitations they impose, in particular the vastly more limited bandwidth and worse latency compared to RAM.

The new SVP challenge record falls in a long line of similar cryptanalytic efforts – affecting real-world cryptographic practice – by cryptanalysts all over the world and at CWI.

The RSA Cryptosystem is the most widely used public-key cryptosystem and its security relies on the hardness of factoring. The RSA factoring challenges were introduced in 1991. The RSA factoring efforts since then have been the benchmark on which RSA key size recommendations are founded even today. CWI has been involved in the RSA factoring challenges since 1993 till 2012 with the retirement of Herman te Riele.

Cryptographic hash functions are another important cryptographic tool and a crucial part of all digital signatures. MD5 and SHA-1 have been industry's de facto standards for many applications, including digital signatures. However, Chinese researchers lead by Prof. Xiaoyun Wang demonstrated in 2004 and 2005 that both MD5 and SHA-1 have significant weaknesses. CWI has been involved in efforts from 2008 till 2017 in studying the graveness of MD5's and SHA-1's weaknesses by significantly improving attacks in practice and demonstrating real world threats. Today's secure hash standards are SHA-2 and a new hash standard SHA-3, published by NIST in 2012 following MD5's and SHA-1's weaknesses.

30 Mar 2021

3 IBM brings its Quantum System One to the Cleveland Clinic

by Frederic Lardinois

https://techcrunch-com.cdn.ampproject.org/c/s/techcrunch.com/2021/03/30/ibm-brings-its-quantum-system-one-to-the-cleveland-clinic/amp/

IBM has installed a couple of its own Quantum System One machines across the world in recent years, but today it announced its first private-sector U.S. deployment thanks to a new 10-year partnership with the Cleveland Clinic. This not only marks IBM's first U.S. install of one of its quantum computers outside of its own facilities, but also the first time a healthcare institute purchases and houses a quantum computer.

And thanks to this deal, Cleveland will also get access to IBM's upcoming next-gen 1,000+ qubit quantum system.

We're still in the very early days of commercializing quantum computing and for most current users, having access to a system over the cloud is sufficient for the experiments they are running. But increasingly, we are seeing research institutes and even some commercial users who are looking to install on-premises quantum computers to have full access to a dedicated machine.

This new deal is part of a larger partnership between IBM and the Cleveland Clinic, which also involves IBM's hybrid cloud portfolio for high-performance computing and its AI tools. The partnership also forms the foundation of Cleveland Clinic's new Center for Pathogen Research & Human Health, which is supported by $500 million in investments from the State of Ohio, Jobs Ohio and Cleveland Clinic.

"What we're announcing here is the first – I'm going to call them private sector or nonprofit – but still, it's the first sort of non-government organization that is going to have not only fully dedicated systems, but what is really, really remarkable is our commitment for the decades," Dario Gil, IBM's SVP and director of IBM Research, told me. "In a way, they are partnering with us for the entire roadmap. So it's not only taking receipt and getting access to a fleet of quantum computers and the next-generation quantum computer for next year. They're also the first ones who are signing up and says, 'I want the first 1,000+ qubit system."

He noted that it takes a very forward-looking organization to invest heavily in quantum computing today. It's one thing for a nation-state to start working with this nascent technology, given the potential it has in a wide variety of fields, but it's another for a nonprofit to make a similar bet. "The level of ambition is really, really high on their end because they're thinking about the future," Gil said of the Cleveland Clinic's leadership.

Gil noted that as part of the overall deal, Cleveland Clinic's researchers will also get access to IBM's entire quantum portfolio in the cloud. IBM will maintain and support the on-premises quantum computer and they will remain IBM-owned machines, similar to its deals with government research labs in Japan and Germany, he explained.

"Maintaining it and supporting it is really critical," Gil said about why that's the case. "And they need us and our expertise to be able to do that. And also, you know, we do it because it's like one of the most sensitive technologies that we have in IBM. So we are exquisitely focused on maintaining the security and safety for the machines."

As part of the overall deal, IBM and Cleveland Clinic will also work on building skills among Cleveland Clinic's researchers in quantum computing, but also AI and high-performance computing.

"Through this innovative collaboration, we have a unique opportunity to bring the future to life," said Tom Mihaljevic, M.D., president and CEO of Cleveland Clinic. "These new computing technologies will revolutionize discovery in the life sciences and ultimately improve people's lives. The Discovery Accelerator will enable our renowned teams to build a forward-looking digital infrastructure and transform medicine, while training the workforce of the future and growing our economy."

4 The Road Ahead: Post-Quantum Cryptography

https://www.isara.com/blog-posts/the-road-ahead-post-quantum-cryptography.html?utm_medium=email&_hsmi=118648974&_hsenc=p2ANqtz--D4bAmQ6D_krJBXFBsugBFQk1cSafxFQyFPMkwJYYmtsL6WnAVcXzLQIZWAJpsaRu-91aWIivN6s16v3ldeV5LjlaolQ&utm_content=118648974&utm_source=hs_email

Are we there yet? If you have traveled on a road trip with children, you probably have been asked this a hundred times. As with any road trip, you likely have done some pre-planning – a full tank of gas, some idea of where you're going, GPS or a map, clothes packed, snacks, music. You are usually somewhat prepared for the journey ahead.

Enterprises and organizations are traveling – not on a mere road trip – but on a considerable journey. Destination: post-quantum cryptography. "There is no greater cryptographic migration than the one which CISOs and CIOs have now started preparing for: from classical, public key cryptography to quantum-safe cryptography," states Paul Lucier, VP of sales, business development and marketing at ISARA, in his recent Security Boulevard article, Your Quantum-Safe Migration Journey Begins with a Single Step.

NIST continues to move forward, as well, with its post-quantum cryptography (PQC) standardization project. Last month, in a presentation to ASC X9 Inc., NIST mathematician, Dustin Moody, Ph.D., outlined the latest happenings with the project and what's on the horizon. He discussed what NIST will be considering when it selects which third-round candidates to standardize, in terms of security, performance, and implementation characteristics. There was also discussion around the need for more real-world tests of the candidate algorithms.

Where is the NIST PQC Standardization Project Today?

Which way? This way. Currently in its third selection round, the cryptographic algorithm finalists and alternates are:

- **KEM finalists:** Kyber, NTRU, SABER, Classic McEliece
- **Signature finalists:** Dilithium, Falcon, Rainbow
- **Alternative KEMS:** BIKE, FrodoKEM, HQC, NTRUprime, SIKE
- **Alternative Signatures:** GeMSS, PICNIC, SPHINCS+

NIST intends to standardize a suite of algorithms. Standardizing a diverse collection of algorithms provides a well-rounded strategy against future cryptanalysis. Since some of these third-round candidates are sufficiently similar to each other, NIST expects to standardize **at most** one of the following:

- KEM: Kyber or NTRU or Saber
  - These are similar, it's likely all three won't be required
- Signature: Dilithium or Falcon
  - They are both based on structured lattices. No need for both
- Both balanced, efficient, lattice-based signature
  - Moody noted that it will be hard to choose one of them

"A wide range of mathematical ideas are represented by these algorithms. Most fall into three large families – lattice, code-based, multivariate," Moody has said. "It's important for the eventual standard to offer multiple avenues to encryption."

The Journey to Post-Quantum Cryptography

How do we get there? Moody offers 12 tips to plan for the journey to PQC:

(i) Perform quantum risk assessment within your organization

(ii) Identify information assets and their current cryptographic protections

(iii) Identify your X, Y, and Z (referring to Mosca's XYZ Theorem)

(iv) Prioritize activities required to maintain awareness

(v) Migrate technology to quantum-safe solutions

(vi) Evaluate vendor products with quantum-safe features

(vii) Know which products are not quantum-safe

(viii) Ask vendors for quantum-safe features in procurement templates

(ix) Develop an internal knowledge base amongst IT staff

(x) Track developments in quantum computing and quantum-safe solutions

(xi) Establish a roadmap to quantum readiness for your organization

(xii) Act now! It will be less expensive, less disruptive, and less likely to have mistakes caused by rushing and scrambling

Enterprises can start preparing now with crypto-agile solutions, as NIST indicates. Crypto-agility can help organizations bridge the gap between current and quantum-safe security. For example, ISARA's Catalyst™ Agile Digital Certificate Methodology enables a cost-effective and simplified migration to quantum-safe security today by supporting two cryptographic algorithms – one classic and one quantum-safe algorithm – within a single X.509 certificate.

Here are resources on crypto-agility and PQC information and migration strategies:

- NIST Post-Quantum Cryptography Standardization outlines an overview, FAQs, news, updates, publications, and presentations
- ETSI QSC Migration Technical Report provides recommendations for quantum-safe schemes
- Quantum-Safe Hybrid Key Exchange Standard published by ETSI
- X9 provides a wide range of quantum computing information, including a report on quantum computing risks
- Managing Cryptographic and Quantum Risk outlines how enterprises can start taking action
- Quantum-Safe Readiness Program for Enterprises is a workshop to gain hands-on experience and explore quantum-safe cryptography

Are we there yet? No! But now is the time to start planning for the post-quantum cryptography migration journey by gaining some familiarity with the new cryptographic algorithms. "By starting now, you will better equip your organization to confront the very real difficulties of the transition, and manage unwelcome surprises that could derail and delay quantum-safe migration efforts and create soaring back-end costs," recommends Lucier. The first stop: inventorying assets and conducting an impact analysis.

In the rear-view mirror, let's look back to 25 years ago. In The Road Ahead, Bill Gates wrote, "The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers." Fast forward to the present, and that vision for the future has become clearer than ever before.

So, pack your bags and prepare your playlists, because the road ahead leads to a quantum-safe enterprise.

25 Mar 2021

5 Detecting photons transporting qubits without destroying quantum information

by Max Planck Society

https://phys.org/news/2021-03-photons-qubits-quantum.html

Even though quantum communication is tap-proof, it is so far not particularly efficient. Researchers at the Max Planck Institute of Quantum Optics want to change this. They have developed a detection method that can be used to track quantum transmissions. Quantum information is sent over long distances in the form of photons (i.e. light particles). However, these are quickly lost. Finding out after only a partial distance whether such a photon is still on its way to its destination or has already been lost, can significantly reduce the effort required for information processing. This would make applications such as the encryption of money transfers much more practicable.

Quantum cryptography could soon become the method of choice to secure the data traffic of government agencies or banks. However, in the foreseeable future, it will probably not protect our email traffic from uninvited readers. The exchange of qubits, the smallest unit of quantum information, is simply far too complex. One of the biggest problems: Light particles that carry qubits over long distances and are easily deflected from their path in the air or absorbed in glass fibers – and suddenly, the quantum information is lost. Because most photons are lost in a transmission over around 100 km, thousands of photons would have to be transmitted in order to directly transmit only a single qubit over this distance. The transmission of quantum information can thus become a lengthy affair, even though light travels very fast and can cover the distance from Munich to Berlin (around 600 km) in only about two milliseconds.

The detector does not read the quantum information

A team around Dominik Niemietz and Gerhard Rempe at the Max Planck Institute of Quantum Optics has now developed a physical protocol that can indicate whether the qubit has gone already lost at intermediate stations of the quantum transmission. "If this is the case, the transmitter can send the qubit again with significantly less delay than if the loss is noticed only at the receiving end," says Dominik Niemietz, who developed the detector for photonic qubits (as it is called in technical jargon) as part of his dissertation. "It is essential that we do not destroy the qubit. We are thus only detecting the qubit photon and not measuring it." In other words: The detector detects whether the photon is there or not but does not read the quantum information encoded into it. It's something like tracking a shipment online without being able to see inside the package. "This is crucial because the laws of quantum physics rule out copying a qubit 1 to 1 – this is what quantum cryptography is based on." Quantum post can thus not be refreshed at an intermediate station – neither by those who installed the transmitter and receiver, nor by spies.

Two resonators and one atom enable the detection of the qubit

In order to detect a photon carrying quantum information without reading the message itself, the physicists work with an atom that they trap in two perpendicular resonators. The two resonators each consist of two mirrors so that the atom is surrounded by four mirrors arranged in a cross. One of the resonators is designed in such a way that the atom recognizes the presence of the photon by an extremely gentle touch: The resonator is located at the end of an optical fiber through which a photon reaches it – or not. When the photon arrives there, it is reflected and changes the state of the atom. What is important here is that the quantum information remains unaffected by this – in much the same way as package deliverers leave messages if the recipients are not home and take the package away again. The photon influences the state of the atom. In the process, the atomic spin is changed – similar to a spinning top, the rotation of which is reversed by 180 degrees from one moment to the next. In contrast, the quantum information is packed into the oscillation plane – physicists speak of polarization – of the photon.

But how can we tell whether the photon was there and changed the state of the atom or not? This is the job of the second resonator. If no photon arrives at the detector at the expected time, the Garching physicists can make the atom glow by irradiating it with laser light. They can easily detect the glow via the second pair of mirrors and with a classical photodetector. If a photon is reflected at the other resonator, changing the state of the atom, this does not work, and the atom remains dark.

From 14 kilometers, the detector accelerates quantum communication

The Max Planck researchers have shown with model calculations that the detection of photons transporting qubits makes quantum communication more efficient. Accordingly, the detector they used for their experiment would accelerate the transmission of quantum information at a greater distance than 14 kilometers. “A detector for photonic qubits can also be useful at shorter distances,” says Pau Farrera, who was part of the research team. However, in order for this to happen, the detection would have to work even more reliably than it did in the current experiment. “This is not a fundamental problem but rather only a technical one,” explains the physicist. The efficiency of the detector currently suffers primarily because the resonator reflects only about one third of the incoming photons. Only in the case of a reflection does a photon leave a trace in the atom. “However, we can increase this efficiency to almost 100 percent by improving the fabrication of the resonators.”

A detector that reliably detects a photonic qubit would not only be helpful in tracking quantum information during transmission but could also confirm the arrival of quantum post at its destination. This is beneficial if the information encoded in the photon is to be further processed in a complex manner – for example, if it is to be transferred to entangled atoms. Entanglement is a quantum mechanical phenomenon that can be used to encrypt and process data. In this process, two spatially widely separated particles become a single quantum entity. Changes in one particle thus directly lead to changes in the other. “Creating entanglement is complex,” says Gerhard Rempe, Director at the Max Planck Institute of Quantum Optics. “You should use it to process a qubit only if you are sure that this qubit is there.”

Demonstrating how quantum post tracking could be used in information processing is a possible goal of future experiments in Gerhard Rempe’s group: “We would like to use the detector for quantum communication between our Institute in Garching and a more distant location. For example, to make the step from our laboratory to practical application,” says the Max Planck Director. “In this way, we are once again getting a little closer to our great long-term goal, the quantum internet.”

6 Application-Motivated, Holistic Benchmarking of A Full Quantum Computing Stack

by Karine

https://www.dailysabah.com/business/tech/beijing-presses-tech-giants-over-deep-fakes-internet-security

Benchmarking of Quantum Computing devices is necessary to measure their performance, and to guide their use and future development. As Quantum Computing systems become more complex, they need to be benchmarked in terms of practical applications they would be expected to do.

A team of researchers at University of Edinburg, Cambridge Quantum Computing and IBM has published a paper which sets out and demonstrates an application-motivated benchmarking framework for full-stack quantum computational systems.

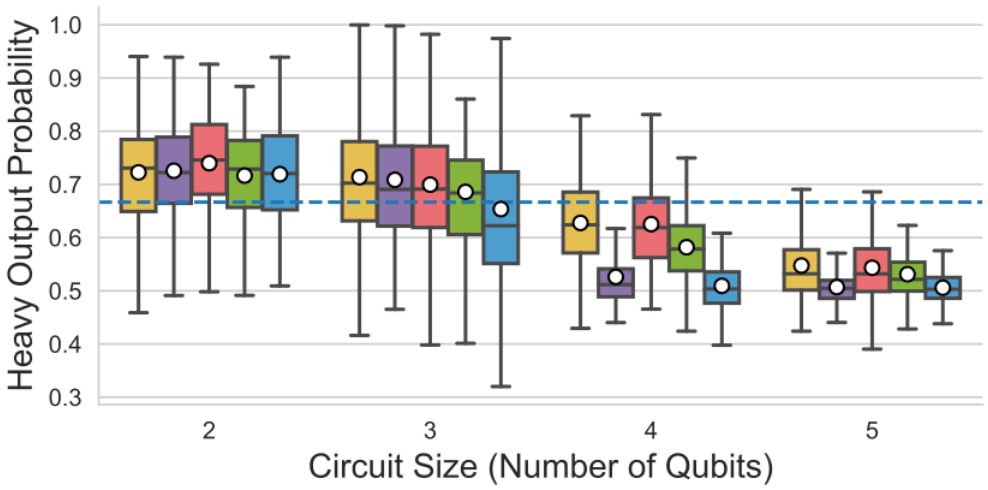


Figure 1: An example comparison of compilation strategies (fixed colours) when used on application-motivated circuits run on a real device.

The framework is used to benchmark the performance of several quantum devices made available by IBM Quantum, which are combined with different compiler strategies (enabled by CQC's tket and IBM's Qiskit) to produce the full-stack.

By considering three different classes of circuits, motivated by a variety of applications, the framework assesses the strengths and weaknesses of quantum computational systems when performing relevant tasks. This work also considers the effect of different noise-aware compilation strategies, which are used to transform and optimise a circuit. Doing so can inform compiler development for a given application or device.

23 Mar 2021

7 Spy Museum Launches Limited-Run Pop-Up Exhibit of Extraordinary Codebreaking Artifacts

https://www.spymuseum.org/press/press-archive/2021-press-releases/spy-museum-launches-limited-ru/

The International Spy Museum (SPY) launches a mini pop-up exhibit, **Codes, Ciphers & Mysteries: NSA Treasures Tell Their Secrets**, from April 5 through May 31 to showcase a select trove of key artifacts used for codemaking, codebreaking, and secure communications. The 13 historic objects are first-of-their-kind, one-of-a-kind, and breakthrough pieces, some of which have played a key role in shaping world history.

The artifacts will be on special display in the Briefing Center where guests begin their visit and will expand upon the Museum's permanent exhibit on Codes. The remarkable items are on loan from the National Cryptologic Museum (NCM), which collects, preserves, and showcases unique cryptologic treasures and serves as the National Security Agency's principal gateway to the public.

"At a time when people are glued to their iPhones, locked in endless Zoom meetings, or wondering what personal information will be hacked next, the public is increasingly curious about the machinery that keeps their communications private and protected," shared Dr. Andrew Hammond, the Historian & Curator at the International Spy Museum. "Partnering with the National Cryptological Museum on this pop-up exhibit allows us to share with our audience some of the secret history of secure communications. Prepare for superstar artifacts, colorful characters, and history-making machines – right here, in the heart of Washington DC."

Several highlights of Codes, Ciphers, & Mysteries are:

- **Cypher Cylinder, late 1700s/early 1800s:** Believed to be the oldest existing true cipher device in the world, this wheel cipher is similar to one designed by Thomas Jefferson.
- **PURPLE Analog No. 1, 1940:** The machine built to crack the Japanese PURPLE code. This machine is responsible for decrypting the famous 14-part message telling the Japanese ambassador to end diplomatic negotiations with the US in advance of the Pearl Harbor attacks.
- **JN-25 Depth Analyzer, 1942:** Used to help US codebreakers crack JN-25, the main Japanese naval code, which allowed the less experienced US Navy to score a decisive victory against Japan at the Battle of Midway. This artifact has never before been seen by the public.
- **Piece of Colossus, 1944:** Colossus was the world's first-ever electronic computer, built by the British to break Germany's sophisticated Lorenz cipher machine.
- **PACE TR-10, 1960:** Believed to be the first desktop analog computer used at NSA. Developed by Electronic Associates Inc. in New Jersey.
- **US Space Shuttle Challenger Encryption System, 1983:** Built by the NSA, this high-level encryption system was collected from the Challenger's debris after it broke apart 73 seconds into its mission.

"The National Cryptologic Museum has been busy redesigning its exhibits and revitalizing its building while we remain closed," shared Dr. Vince Houghton, Director of the National Cryptologic Museum. "As

we continue to pursue our goal to reopen in the summer, we've loaned the International Spy Museum some of the rarest, oldest, most historically significant code and cipher artifacts in the world."

When the pop-up closes on May 31, the artifacts will return to the National Cryptologic Museum at Ft. Meade, Maryland. NCM expects to reopen to the public this summer.

For photo, information, or filming inquiries related to the Spy Museum's new mini pop-up exhibit, please contact Aliza Bran at 202.654.0946 or abran@spymuseum.org.

22 Mar 2021

8 The Pillars of Future Cryptography at IBM

by Sergio De Simone

https://www.infoq.com/news/2021/03/future-cryptography-ibm/

In a recent webinar, IBM summarized the latest advances in cryptographic technologies the company has been working on, including confidential cryptography, quantum-safe encryption, and fully homomorphic cryptography.

According to Gosia Steinder, IBM hybrid cloud research CTO, each of those technologies is solving a different piece of the security equation.

Confidential computing is IBM moniker for security enclave-based cryptography in the cloud:

> Confidential computing provides hardware-level privacy assurance by encrypting data within a secure enclave that not even the cloud provider can view or access.

This enables users to run workloads in the cloud or on-premises with the maximum privacy and control even when they don't own the infrastructure they are using, says Hillery Hunter, IBM VP and CTO of IBM Cloud.

Confidential computing is not only relevant to guarantee data privacy on the Cloud, but also to ensure data integrity and to prevent anyone from tampering with the data, says Samuel Brack, CTO of open-source financial platform DIA. The alternative to using confidential cryptography would be a decentralized approach with increased costs and reduced performance, he adds.

Looking at the future, quantum computing is known to pose a serious challenge to cryptography, says IBM cryptography researcher Vadim Lyubashevsky. As he explains, some of today's cryptography is based on factoring, a problem which is considered hard on classical computers but quantum computers can effectively solve. For example, says Lyubashevsky, a prime integer with a thousand digits could require billions of years to be factored on classical hardware, while a quantum computer could in a couple of hours.

A particularly worrisome dimension of this is highlighted by Dustin Moody, mathematician at NIST, who is working at defining standards for post-quantum cryptography. Indeed, while quantum hardware is not yet there, the mere possibility of its existence means encrypted data is potentially under a threat of attack now. In fact, somebody could take hold of that data and wait for quantum hardware to be available to decrypt it. As a consequence of this, he says, you may not be protecting your data for the amount of time you hope you do.

As Moody recounts, NIST is running an open process to select the best crypto systems, based on security and performance. Currently there are seven encryption schemes that advanced to round 2 in the selection process, out of 69 initial competitors. The expectation is to be able to have a draft standard for the first quantum resistant algorithms at the beginning of 2022, with the prospect of completing its standardization by 2024 after a process of public comment.

Transition will not be easy, though, says Moody:

> We're dealing with algorithms that are a lot more complex in terms of the math they use and some of the characteristics that they have also have things like larger key sizes so we as much as possible are trying to prepare as much as we can and encourage others to do so.

Four of the quantum-safe algorithms that made it to phase 2 were initially proposed by IBM, highlights Lyubashevsky, and they are available through the open source Cryptographic suite for algebraic lattices (CRYSTALS).

> These schemes derive their security from the fact that they are based on the presumed algorithmic hardness of something called lattice problems.

In other words, counter to integer factoring, lattice problems are thought to be hard even for quantum computers. To understand what lattice problems look like, Lyubashevsky suggests a simple example. Say you have a public list of six numbers. You pick three of them and then calculate their sum. The problem consists in finding which three numbers you chose from their sum. When you deal with thousands of thousand-digit numbers, it seems this problem would be hard for quantum computers. Lattice problems are just one possible approach to post-quantum cryptography.

As mentioned, IBM is providing an implementation for CRYSTALS, which makes it possible to carry through experiments to assess their performance.

> We've noticed that the efficiency of the schemes is such that the end user won't notice any difference. In fact, sometimes the new scheme is even faster. So, the quantum threat is not an existential one for cryptography. We will have security.

According to Lyubashevsky, there is no reason to wait further before switching to lattice cryptography using CRYSTALS. The critical point would be not to hard-code the scheme you use but make it replaceable as a black box. In this way, you are prepared for when standardized quantum-safe schemes become eventually available.

The final front on which IBM is working regarding cryptography is fully homomorphic encryption, which brings the promise of enabling computing data while in its encrypted form. This makes away with the need to decrypt the data before processing it, which leaves it in a vulnerable and exposed state.

IBM FHE has made great advances from its inception to the initial implementation in 2011, which was painfully slow, to 2015, when it became possible to compare two fully encrypted genomes with FHE in less than an hour. FHE is today ready to be used by any companies, from small to large, says IBM.

Eric Maass, strategy and emerging technology director at IBM, explains that FHE is made possible by some of the same lattice encryption techniques and mathematics used in CRYSTALS.

> Adopting FHE in a more widespread manner has been historically complex not just in terms of the calculations that are performed on the data. It also requires a lot of computing power and the skills and learning curve have typically been very steep.

While confidential cryptography is a rather mature technology, homomorphic encryption and post-quantum cryptography are research fields that still attract lots of efforts. IBM is not the only company investing on homomorphic encryption. Microsoft, for instance, released SEAL (Simple Encrypted Arithmetic Library), and Google recently unveiled its Private Join and Compute tool. Similarly, a number of efforts towards quantum-safe computing are ongoing at several other companies, including Google, which selected NewHope, Microsoft, with PICNIC, and others.

19 Mar 2021

9 Free Open-Access Quantum Computer Now Operational

by sandia national laboratories

https://scitechdaily.com/free-open-access-quantum-computer-now-operational/

Scientists worldwide can use ion-based testbed at Sandia National Laboratories.

A new Department of Energy open-access quantum computing testbed is ready for the public. Scientists from Indiana University recently became the first team to begin using Sandia National Laboratories' Quantum Scientific Computing Open User Testbed, or QSCOUT.

Quantum computers are poised to become major technological drivers over the coming decades. But to get there, scientists need to experiment with quantum machines that relatively few universities or companies have. Now, scientists can use Sandia's QSCOUT for research that might not be possible at their home institutions, without the cost or restrictions of using a commercial testbed.

"QSCOUT serves a need in the quantum community by giving users the controls to study the machine itself, which aren't yet available in commercial quantum computing systems. It also saves theorists and scientists from the trouble of building their own machines. We hope to gain new insights into quantum performance and architecture as well as solve problems that require quantum computation," said Sandia physicist and QSCOUT lead Susan Clark.

She said the new testbed is a rare machine in three ways:

- first, as a free, open-access testbed;
- second, as one made with trapped ion technology; and
- third, as a platform that gives users an uncommon amount of control over their research.

Last month, Sandia began running the testbed's first user experiment for scientists from Indiana University. Researchers from IBM, Oak Ridge National Laboratory, the University of New Mexico and the University of California, Berkeley, have also been selected to begin experiments soon. Their projects range from testing benchmarking techniques to developing algorithms that could someday solve problems in chemistry too complex for normal computers.

Researchers interested in using the **Quantum Scientific Computing Open User Testbed** are invited to sign up for notifications by emailing qscout@sandia.gov. Sandia expects to select the next round of projects in the spring, subject to change.

Sandia soliciting proposals

Now, Sandia is getting ready for more research proposals. Anyone can submit a proposal to use QSCOUT, and computing time is free thanks to funding from the DOE Office of Science, Advanced Scientific Computing Research program. The next group of projects is expected to be selected in the spring.

On top of providing an exceptional research opportunity, QSCOUT has a rare design for a testbed. Most commercial testbeds use technology called superconducting circuits. Such machines need to be kept at ultralow temperatures, making them expensive to build and operate. But Sandia's testbed uses what is called an ion trap instead. This means Sandia's testbed can run at warmer temperatures. Trapped ions also yield clearer signals than circuits and hold on to information longer, enabling scientists to perform different types of experiments and compare the two platforms.

Trapped ions are held inside QSCOUT in a so-called "**trap on a chip**," a flat, bow tie-shaped device, about 2 cm (0.8 inches) long, overlaid on a semiconductor chip. Three electrically charged atoms of the element ytterbium are suspended in place by radio waves and an electric field above a hairline channel that runs down the center of the device. Lasers encode information in each ion as a qubit, comparable to a bit in a conventional computer, to perform calculations.

Sandia plans to expand the system from three to 32 qubits over the next three years so scientists can perform more sophisticated tests.

QSCOUT resides at Sandia's Microsystems Engineering, Science, and Applications complex, which also produces microelectronics for the nation's nuclear stockpile.

10 Solving 'barren plateaus' is the key to quantum machine learning

by Los Alamos National Laboratory

https://phys.org/news/2021-03-barren-plateaus-key-quantum-machine.html

Many machine learning algorithms on quantum computers suffer from the dreaded "barren plateau" of unsolvability, where they run into dead ends on optimization problems. This challenge had been relatively unstudied – until now. Rigorous theoretical work has established theorems that guarantee whether a given machine learning algorithm will work as it scales up on larger computers.

"The work solves a key problem of useability for quantum machine learning. We rigorously proved the conditions under which certain architectures of variational quantum algorithms will or will not have barren plateaus as they are scaled up," said Marco Cerezo, lead author on the paper published in Nature Communications today by a Los Alamos National Laboratory team. Cerezo is a post doc researching quantum information theory at Los Alamos. "With our theorems, you can guarantee that the architecture will be scalable to quantum computers with a large number of qubits."

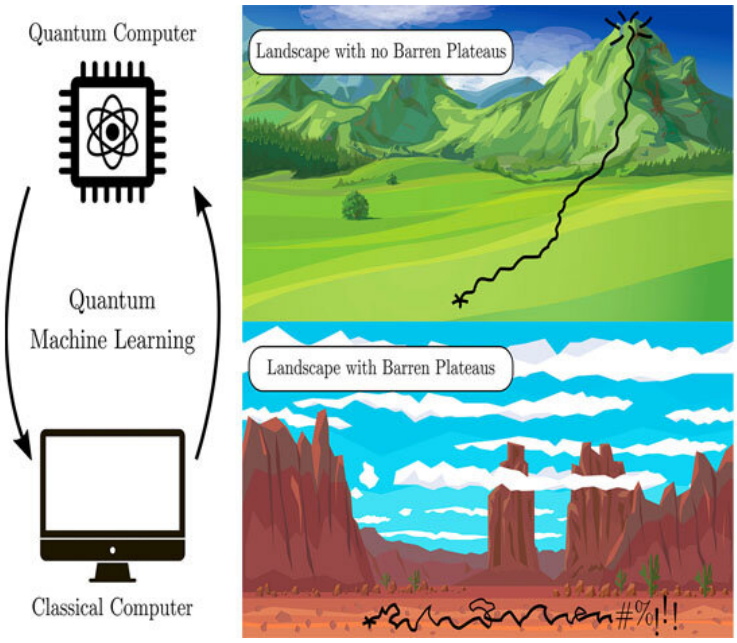


Figure 2: A barren plateau is a trainability problem that occurs in machine learning optimization algorithms when the problem-solving space turns flat as the algorithm is run. Researchers at Los Alamos National Laboratory have developed theorems to prove that any given algorithm will avoid a barren plateau as it scales up to run on a quantum computer.

"Usually the approach has been to run an optimization and see if it works, and that was leading to fatigue among researchers in the field," said Patrick Coles, a coauthor of the study. Establishing mathematical theorems and deriving first principles takes the guesswork out of developing algorithms.

The Los Alamos team used the common hybrid approach for variational quantum algorithms, training and optimizing the parameters on a classical computer and evaluating the algorithm's cost function, or the measure of the algorithm's success, on a quantum computer.

Machine learning algorithms translate an optimization task – say, finding the shortest route for a traveling salesperson through several cities – into a cost function, said coauthor Lukasz Cincio. That's a mathematical description of a function that will be minimized. The function reaches its minimum value only if you solve the problem.

Most quantum variational algorithms initiate their search randomly and evaluate the cost function globally across every qubit, which often leads to a barren plateau.

"We were able to prove that, if you choose a cost function that looks locally at each individual qubit, then we guarantee that the scaling won't result in an impossibly steep curve of time versus system size, and therefore can be trained," Coles said.

A quantum variational algorithm sets up a problem-solving landscape where the peaks represent the high energy points of the system, or problem, and the valleys are the low energy values. The answer lies in the deepest valley. That's the ground state, represented by the minimized cost function. To find the solution, the algorithm trains itself about the landscape, thereby navigating to the low spot.

"People have been proposing quantum neural networks and benchmarking them by doing small-scale simulations of 10s (or fewer) few qubits," Cerezo said. "The trouble is, you won't see the barren plateau with a small number of qubits, but when you try to scale up to more qubits, it appears. Then the algorithm has to be reworked for a larger quantum computer."

A barren plateau is a trainability problem that occurs in machine learning optimization algorithms when the problem-solving space turns flat as the algorithm is run. In that situation, the algorithm can't find the downward slope in what appears to be a featureless landscape and there's no clear path to the energy minimum. Lacking landscape features, the machine learning can't train itself to find the solution.

"If you have a barren plateau, all hope of quantum speedup or quantum advantage is lost," Cerezo said.

The Los Alamos team's breakthrough takes an important step toward quantum advantage, when a quantum computer performs a task that would take infinitely long on a classical computer. Achieving quantum advantage hinges in the short term on scaling up variational quantum algorithms. These algorithms have the potential so solve practical problems when quantum computers of 100 qubits or more become available – hopefully soon. Quantum computers currently max out at 65 qubits. A qubit is the basic unit of information in a quantum computer, as bits are in a classical digital computer.

"The hottest topic in noisy intermediate-scale quantum computers is variational quantum algorithms, or quantum machine learning and quantum neural networks," Coles said. "They have been proposed for applications from solving the structure of a molecule in chemistry to simulating the dynamics of atoms and molecules and factoring numbers."

18 Mar 2021

11 Quantum computing breaking into real-world biz, but not yet into cryptography

by Eileen Yu

https://www.zdnet.com/article/quantum-computing-breaking-into-real-world-biz-but-not-yet-into-cryptography/

Quantum computing is ready for mainstream deployment, where it already is being tapped to resolve real-world business challenges. Use of the technology to crack cryptography and encryption codes, however, still has some ways to go.

In particular, D-Wave Systems CEO Alan Baratz believes it can take at least another decade before factoring will be viable on quantum computing systems and used to undermine current cryptographic tools.

And this was likely the case whether the gate-based system, along with its volatile error correction, or D-Wave's annealing technology was tapped to factor the large code volumes used in cryptography tools, Baratz said in a video call with ZDNet.

That said, D-Wave had an internal security team that monitored activities on its systems, he revealed, whilst acknowledging that it was still too soon to determine the types of hacking tools that could or had been created on quantum computers.

The Canadian quantum computing vendor does not specifically focus on cryptography, but its technology has been used to power intrusion and threat detection applications. It also has presence in the US, UK, and Japan, where it has 20 paying customers in the Asian market. Its cloud-based Leap quantum computing application is available in Singapore.

A Deloitte Consulting report echoed Baratz's views, stating that quantum computers would not be breaking cryptography or run at computational speeds sufficient to do so any time soon. However, it said

quantum systems could pose a real threat in the long term and it was critical that preparations were carried out now to plan for such a future.

On its impact on Bitcoin and blockchain, for instance, the consulting firm estimated that 25% of Bitcoins in circulation were vulnerable to a quantum attack, pointing in particular to the cryptocurrency that currently were stored in P2PK (Pay to Public Key) and reused P2PKH (Pay to Public Key Hash) addresses. These potentially were at risk of attacks as their public keys could be directly obtained from the address or were made public when the Bitcoins were used.

Deloitte suggested a way to plug such gaps was post-quantum cryptography, though, these algorithms could pose other challenges to the usability of blockchains. Adding that this new form of cryptography currently was assessed by experts, it said: "We anticipate that future research into post-quantum cryptography will eventually bring the necessary change to build robust and future-proof blockchain applications."

Mathematician Peter Shor in 1994 published a quantum formula that he said could break most common algorithms of asymmetric cryptography. It suggested that, given a large enough quantum computing system, the algorithm could be used to identify a private key that matched its corresponding public key to impersonate digital signatures.

A team of engineers and researchers in Singapore last year also announced plans to tap quantum cryptography technology to enhance network encryption tools, so these could be ready to mitigate security risks when quantum computing became mainstream. Specifically, they were looking to use "measurement-device-independent" quantum key distribution (MDI QKD) technology and hoped to their research could pave the way to a new class of "quantum-resilient encryptors".

quantum ready for mainstream enterprise application

While the technology has yet to break cryptography, quantum computing is ready for mainstream adoption and already is tapped to address real-world enterprise challenges.

Pointing specifically to D-Wave's proprietary annealing technology, Baratz said this allowed quantum computing to scale more easily and be less sensitive to noise and computational errors, to which gate-based systems were prone. Currently in its fifth generation, D-Wave's quantum computers clock more than 5,000 qubits and capable of supporting commercial rollout "at commercial scale", he said.

This, he added, was a stage that no other market players had been able to achieve thus far with the gate-based model. Commonly adopted in the industry today, the gate system made quantum computers tough to build and sensitive error. Its most stable state currently generated about 30 qubits, which was sufficient to power mostly research work and unlikely to be used to solve business problems at scale for another seven to 10 years, he said.

"Error rates on [gate-based systems] are so high you can't really do anything with them, even with small problems," he added, noting that a competitor last year said it was able to solve a specific optimisation problem on its quantum computer. However, this was possible once out of every 100,000 attempts, he said.

Quantum computing runs on principles of quantum mechanics that include probabilistic computation.

Baratz said annealing technology, designed specifically for optimisation purposes, had a higher influence on the probability of outcomes and, hence, was less sensitive to errors. It also learnt from where it ended with the previous computation to finetune future ones.

"When you lose coherence, you end up with garbage. With annealing, when you lose coherence, you

settle into a [potential] solution and restart the computation to try and improve the solution," he said. Gate-based model, in comparison, could not do that since it would lose coherence after every computation rather than pick off from the previous run.

A grocery using D-Wave to enhance a portion of the customer's logistics system was able to solve an optimisation problem in two minutes per week per location, where previously it took 25 hours per week per location, he noted.

There currently are more than 20,000 developers worldwide that have signed up to access Leap, with some 1,000 regularly using the service each month. Paying customers fork out an estimated $2,000 an hour to run computations on D-Wave computers.

Baratz noted, though, that its systems could not solve all quantum computing issues because annealing was designed specifically to solve optimisation problems, which were common challenges for businesses. Gate-based systems, on the other hand, would be able to solve any computation problems once the error rates were reduced – something he said likely would not actualise for at least another seven years.

So while D-Wave's annealing-powered quantum computers were limited to solving optimisation problems, they were capable of addressing real-world business challenges today, he said. Its systems also were on a path towards building a universal error correction system by leveraging the technology it had, he added.

To date, more than 250 applications had been built with D-Wave systems, most of which used Leap and spanned various use cases including financial modelling, scheduling, protein folding, and manufacturing optimisation, the vendor said.

12 Beijing presses tech giants over 'deep fakes,' internet security

by french press agency

https://www.dailysabah.com/business/tech/beijing-presses-tech-giants-over-deep-fakes-internet-security

Chinese authorities said Thursday they had summoned 11 tech companies – including Tencent, Alibaba and TikTok owner ByteDance – for talks on "deep fakes" and internet security, as regulators try to reel in the country's runaway digital sector.

The Cyberspace Administration of China (CAC) said talks concerned "voice software that has yet to undergo safety assessment procedures" as well as the application of "deep fake" technology.

It also said companies should report to the government plans to add new functions that "have the ability to mobilize society."

China has in recent months taken a tough line on the country's fast-growing tech firms, with 12 companies hit with fines last week for allegedly flouting monopoly rules.

Authorities last year halted a record $34 billion initial public offering by Alibaba fintech subsidiary Ant Group.

They called in its billionaire founder Jack Ma and then opened an investigation into Alibaba business practices deemed anti-competitive.

The latest summoning of big tech also involves companies such as smartphone maker Xiaomi, TikTok rival Kuaishou and music streaming service NetEase Cloud Music, the CAC said.

The aim is to ensure they comply with regulations, carry out safety assessments and take “effective rectification measures” if potential hazards are found.

In 2019, China issued rules banning online video and audio providers from using artificial intelligence (AI) and virtual reality technologies to produce “fake news.”

”Fake news” has been generalized to mean anything from a mistake to a parody or a deliberate misinterpretation of facts.

Regulations stress the dangers of “deep fakes,” meaning technology that manipulates videos to appear genuine but depicts events or speech that never happened.

The CAC notice comes shortly after China blocked the U.S. invite-only audio app Clubhouse.

The app briefly flickered in the mainland before vanishing but has since sparked a number of copycats.

President Xi Jinping on Monday warned about risks surrounding “platform” companies, a term that could refer to mobile and internet firms, and called for greater oversight of the sector.

13 Pioneering Experiment Turns IBM’ s Largest Quantum Computer Into a Quantum Material

by louise lerner

https://scitechdaily.com/pioneering-experiment-turns-ibms-largest-quantum-computer-into-a-quantum-material/

In a groundbreaking study published in Physical Review Research, a group of University of Chicago scientists announced they were able to turn IBM’s largest quantum computer into a quantum material itself.

They programmed the computer such that it turned into a type of quantum material called an exciton condensate, which has only recently been shown to exist. Such condensates have been identified for their potential in future technology, because they can conduct energy with almost zero loss.

“The reason this is so exciting is that it shows you can use quantum computers as programmable experiments themselves,” said paper co-author David Mazziotti, a professor in the Department of Chemistry, the James Franck Institute and the Chicago Quantum Exchange, and an expert in molecular electronic structure. “This could serve as a workshop for building potentially useful quantum materials.”

For several years, Mazziotti has been watching as scientists around the world explore a type of state in physics called an exciton condensate. Physicists are very interested in these kinds of novel physics states, in part because past discoveries have shaped the development of important technology; for example, one such state called a superconductor forms the basis of MRI machines.

Though exciton condensates had been predicted half a century ago, until recently, no one had been able to actually make one work in the lab without having to use extremely strong magnetic fields. But they intrigue scientists because they can transport energy without any loss at all – something which no other material we know of can do. If physicists understood them better, it’s possible they could eventually form the basis of incredibly energy-efficient materials.

To make an exciton condensate, scientists take a material made up of a lattice of particles, cool it down to below -270 degrees Fahrenheit, and coax it to form particle pairs called excitons. They then make the pairs become entangled – a quantum phenomenon where the fates of particles are tied together. But this

is all so tricky that scientists have only been able to create exciton condensates a handful of times.

"An exciton condensate is one of the most quantum-mechanical states you can possibly prepare," Mazziotti said. That means it's very, very far from the classical everyday properties of physics that scientists are used to dealing with.

Enter the quantum computer. IBM makes its quantum computers available for people around the world to test their algorithms; the company agreed to "loan" its largest, called Rochester, to UChicago for an experiment.

Graduate students LeeAnn Sager and Scott Smart wrote a set of algorithms that treated each of Rochester's quantum bits as an exciton. A quantum computer works by entangling its bits, so once the computer was active, the entire thing became an exciton condensate.

"It was a really cool result, in part because we found that due to the noise of current quantum computers, the condensate does not appear as a single large condensate, but a collection of smaller condensates," Sager said. "I don't think any of us would have predicted that."

Mazziotti said the study shows that quantum computers could be a useful platform to study exciton condensates themselves.

"Having the ability to program a quantum computer to act like an exciton condensate may be very helpful for inspiring or realizing the potential of exciton condensates, like energy-efficient materials," he said.

Beyond that, just being able to program such a complex quantum mechanical state on a computer marks an important scientific advance.

Because quantum computers are so new, researchers are still learning the extent of what we can do with them. But one thing we've known for a long time is that there are certain natural phenomena that are virtually impossible to model on a classical computer.

"On a classical computer, you have to program in this element of randomness that's so important in quantum mechanics; but a quantum computer has that randomness baked in inherently," Sager said. "A lot of systems work on paper, but have never been shown to work in practice. So to be able to show we can really do this – we can successfully program highly correlated states on a quantum computer – is unique and exciting."

14 8 Top Quantum Technology Startups In India

by Srishti Deoras

https://analyticsindiamag.com/8-top-quantum-technology-startups-in-india/

In the 2020 budget, the India government allocated ₹8000 crores towards the National Mission on Quantum Technologies and Applications. The fledgeling research field has shown remarkable growth in the last few years. Thanks to the strong support in funding and infrastructure to boost quantum computing growth from the government, many private players are making inroads into the domain.

Here, we have listed a few startups leading the quantum computing race in India.

The list is in no particular order.

(i) **BosonQ**

Founded in 2021, Bhilai-based BosonQ's name is a homage to Indian physicist Dr Satyendra Nath Bose. The startup is building technical infrastructure with a vision to create premier multiphysics simulation software for quantum computing. BosonQ develops world-class quantum computing software solutions, including but not limited to computational fluid dynamics, computational structural dynamics, computational heat transfer, multidisciplinary optimisation, and computational aeroacoustics.

Founded by Abhishek Chopra, BosonQ aims to be a global leader in the quantum computing space.

(ii) **Qulabs.ai**

Qulabs was one of the first quantum computing startups in India. Founded in 2017, the startup aims to provide services in quantum machine learning, quantum communication, quantum computations, quantum algorithms and simulations, etc. With a multidisciplinary group of research scientists and engineers from IITs, ISI and IISc, the Qulabs is pushing the quantum research frontiers in India.

The startup has also set up QuAcademy to provide training, development and translation of new quantum technologies.

(iii) **QpiAI Tech**

Bengaluru-based QpiAI tech is an AI-enabled quantum model generation platform as a service (PaaS) advancing the research efforts in computing and modelling, i.e., bits, neurons and qubits. QpiAI's quantum computing efforts drive innovations in industries such as life sciences, financial services, transport, industry 4.0, space, among others. QpiAI tech has created special optimisation hardware to solve the problem of model complexity.

The startup is inventing hybrid classical-quantum computers in the form of ASGP, AI System Generating Processor. QpiAI relies on CMOS-based quantum dots to fabricate hybrid chips which work at Cryogenic temperature and use current semiconductor processes. Founded by Nagendra Nagaraja, the company aims to put 1 million qubits on a chip to address AI/ML model generation problems.

(iv) **QNu Labs**

Bengaluru-based QNu Labs is a leader in quantum-safe cryptography products and solutions that deals with Quantum Key Distribution (QKD). The tech enables the exchange of cryptographic key between two people with encoded quantum bits, also called Qubits. With its unique offerings, the company provides unconditional and forward security of data on the internet and cloud.

QNu Labs provides quantum random number generator, quantum key generation, quantum key distribution and management solutions across various industries. The startup also provides solutions to ensure customers upgrade their legacy crypto infrastructure to quantum-safe crypto without disrupting their business. QnU has plans to foray into QRNG (Quantum Random Number Generator).

(v) **Automatski**

With offices across Bengaluru and Los Angeles, Automatski performs research in multiple areas, including quantum computing. Some of its remarkable works include circuit quantum computers, adiabatic quantum computers and annealing quantum computers. The startup works in several areas of quantum-inspired software to simulate various quantum computing configurations. It allows simulating configurations with large qubit counts.

Automatski released the world's most powerful 100,000+ Qubits adiabatic quantum computer and quantum annealing quantum computer in 2018. The company has also put unified scale simulations in production the same year, surpassing its earlier billion entity multi-scale simulations capability.

(vi) **Quantica Computacao**

The Chennai-based startup is developing an emerging quantum artificial intelligence platform with the primary objective of developing a software platform to utilise future quantum computer technology. Quantica develops essential software tools, algorithms and components that help with the development of quantum computers. The firm focuses on developing quantum cryptographic tools to provide quantum-proof data security. Other areas of focus include quantum machine learning and artificial intelligence. Quantica is also developing algorithms to address different real-time computing and data analytics challenges.

With Alchemy, the quantum virtual simulator, the company is developing a state of the art quantum virtual simulator to compile and run different quantum capable software tools. It has created a single qubit alpha test version currently and is looking to update the simulator to a four qubit one.

(vii) **QRDLab**

Kolkata-based QRDLab is an industry-first initiative to promote quantum research, education and consulting in multiple areas of quantum computing. With a primary objective of pursuing high-end research in several quantum-inspired software areas, the startup aims to solve various real-life problems.

QRDLab is collaborating with independent researchers and academic institutions to accelerate quantum research. The effort includes t ranslating nascent research ideas and advancing the entire Quantum Computing technology stack in India. The startup's long-term goals include: developing a quantum-based hybrid cryptographic solution for defence, banking, finance and cybersecurity industries; develop a quantum machine learning algorithm for drug discovery: promote quantum education etc.

(viii) **Taqbit Labs**

Founded in 2018, Taqbit Labs is one of the leading startups in quantum tech in India. It offers solutions in the deep technology area of quantum key distribution. Quantum-based encryption is not based on a mathematical or predictable model or any algorithm. Instead, it is guaranteed by quantum physics. The encryption is random, which makes it hack-proof. The focus areas of Taqbit include solving QKD's distance limitations, reliability problems and point-to-point transmission capabilities.

Taqbit's technology has been tested and approved by leading government and scientific institutions. It aims to enhance security and data communication by integrating modern quantum technology within an existing infrastructure. Its application areas include aerospace, defence, manufacturing, finance & healthcare sectors.

15 Quantum Computing Startup IonQ To Go Public: Why Does It Matter?

by Shraddha Goled

https://analyticsindiamag.com/quantum-computing-startup-ionq-to-go-public-why-does-it-matter/

US startup IonQ has entered into a definitive merger agreement with a publicly traded special purpose acquisition company, dMY Technology Group III. The deal will result in $650 million in gross proceeds, including a $350 million fully committed PIPE (private investment in public equity) with participation from Fidelity Management & Research Company LLC, Silver Lake, Breakthrough Energy Ventures, MSD Partners, LP, Hyundai Motor Company and Kia Corporation, etc. The spac deal will put the evaluation of the combined company at around $2 billion.

In a statement, IonQ's spokesperson said, "IonQ believes the 21st century will be defined by quantum computing and that this technology will have an even greater impact than classical computing had over the last 100 years."

IonQ's Products & Future Roadmap

Generally, quantum hardware developers use synthetic quantum systems such as supercooled superconducting wire for qubits. However, IonQ uses trapped ions, which form the heart of their quantum processing units. Using this approach, IonQ has developed the first quantum computer available via the cloud on Amazon Bracket and Microsoft Azure.

In October last year, IonQ introduced a new quantum computer, claimed to be the 'most powerful on the market'. This quantum computer, built on IBM's quantum benchmark, features '32 perfect qubits with low gate errors'. The IonQ claims that the computer is expected to hit a quantum volume extraordinarily higher than the double-digit quantum volume numbers announced by IBM in August 2020.

IonQ has also revealed its plan to build modular quantum computers by 2023 as part of its five-year roadmap. IonQ aims to achieve a broad quantum advantage by 2025.

Quantum Computing Ecosystem

As per an AIMultiple report, Quantum computing companies can be categorised into four types:

- **End-to-end solution providers:** These companies allow others to test quantum solutions on the cloud. Tech giants such as IBM, Google, Microsoft, and D-Wave belong to this category.
- **Software and services companies:** Quantum software providers deliver solutions using quantum computing. These companies can be further classified in terms of their services–operating systems and firmware, development platforms, and computational platforms. Examples include Zapata, Qbit, and Cambridge Quantum Computing.
- **Research Labs:** These are the labs founded as a result of university-industry collaborations. Some of these labs include Institute for Quantum Information and Matter-Caltech, Quantum Computing Laboratory- MIT Lincoln Laboratory, and UK National Quantum Technologies Programme.
- **Hardware system builders:** These companies work on optimising quantum computers and create environments for simulations. They can be further classified into Universal gate based quantum computers and quantum annealing. IonQ is a prime example of this category.

Quantum computing has seen significant advancements, which has drastically reduced the time and effort required to carry out complex tasks, which classical computers cannot accomplish. Experts believe quantum computing will revolutionise science and industry, battery technology, and clean energy.

Bigger companies such as IBM and Google have increased their investment in developing their quantum computing technologies. Investors are also showing interest in the technology. However, there is still a shortage of public pure-play quantum computing companies; most are either private or owned by larger companies.

The arrival of IonQ in this niche market opens up a lot of opportunities. Niccolo de Masi, CEO of dMY III said, "IonQ's quantum computers are uniquely positioned to capture a market opportunity of approximately $65 billion by 2030."

He said IonQ is poised to be the first company able to fully exploit this massive opportunity.

17 Mar 2021

16 Sweden's Quantum Computer Project Shifts up a Gear and Sets Higher Goals

by chalmers university of technology

https://scitechdaily.com/swedens-quantum-computer-project-shifts-up-a-gear-and-sets-higher-goals/

Knut and Alice Wallenberg Foundation is almost doubling the annual budget of the research initiative Wallenberg Centre for Quantum Technology, based at Chalmers University of Technology, Sweden. This will allow the center to shift up a gear and set even higher goals – especially in its development of a quantum computer. Two international workshops will kick-start this new phase.

"Quantum technology has enormous potential and it is important that Sweden has the necessary skills in the area. During the short time since the center was founded, WACQT has built up a qualified research environment, established collaborations with Swedish industry and succeeded in developing qubits with proven problem-solving ability. We can look ahead with great confidence at what they will go on to achieve," says Peter Wallenberg Jr, Chair Knut and Alice Wallenberg Foundation.

Since 2018, Chalmers University of Technology has been managing a large, forward-thinking research initiative – the Wallenberg Centre for Quantum Technology (WACQT) – setting Sweden on course to global prominence in quantum technology. The main project is to develop and build a quantum computer, offering far greater computing power than today's best supercomputers.

During the first three years, the quantum computer researchers within WACQT have focused first on making the basic building blocks of the quantum computer - the qubits - work as well as possible, at small scale. A milestone was reached in 2020, when they managed to solve a small part of a real-world optimization problem with their well-functioning two-qubit quantum computer.

Increases the quality of the hundred qubits

Now comes the time to significantly scale up the number of qubits, and increase the efforts on developing software and algorithms. At the same time, the entire research initiative is being scaled up, with Knut and Alice Wallenberg Foundation (KAW) deciding to almost double WACQT's annual budget, from SEK 45 to 80 million per year for the coming four years. The investment has previously also been extended from its original ten years to twelve, and has now a total funding of at least SEK 1.3 billion including contributions from industry and the participating universities.

"It is very encouraging that KAW shows such great confidence in us. It strengthens WACQT's research program and gives us the opportunity to build an even better quantum computer. In terms of the number of qubits, the goal is still one hundred, but now we are aiming at one hundred really high-performance qubits," says Per Delsing, director of WACQT and Professor at Chalmers.

Calculations have shown that the performance of the final quantum computer will benefit more from increasing the quality of the individual qubits, rather than the total number of qubits. The better their quality , the more useful the final quantum computer.

With the increased funding, WACQT will, among other things, invest in improving the materials in the superconducting chips that constitute the qubits. Quantum states are extremely sensitive, and the slightest disturbance in the materials can impair performance. The qubits manufactured at Chalmers are already among the best in the world, so improving them entails moving the entire research field into new territory.

"These disturbances are extremely small. It requires research just to understand what they are and which are most common. We need to study the entire manufacturing process in detail and explore new ways to eliminate disturbances in the material," Delsing explains.

Will employ another 40 researchers

With the increased funding, the number of researchers working in the quantum computer project can now be significantly increased. For example, a new team will be formed to study nanophotonic devices that can enable the interconnection of several smaller quantum processors into a large quantum computer. Within the next two years, the research force will be expanded by 40 people, almost double the current amount. In a first step, fifteen new postdocs will be recruited.

"This is an ambitious recruitment in a highly competitive niche area. But our hopes are high – through previous recruitments, we have attracted top talents both from Sweden and internationally. We have a unique interaction with the industry, extensive experience of superconducting circuits and an amazing cleanroom facility," says Delsing.

To mark the quantum computer project's new, next-level development, WACQT is organizing two international workshops: one on quantum software and optimization (April 8-9), and the second on enabling technology and algorithms for quantum computing (April 13-14). Anyone curious to hear about the state of the art in quantum computing can follow the workshops online.

"These are very exciting times in quantum computing. New steps are being taken all the time and the competition is rapidly increasing, with many countries making major investments. This investment will ensure that Sweden and Chalmers remain at the global forefront," Delsing says.

17 Microsoft-Backed Quantum Computer Research Retracted

by Charles Q. Choi

https://spectrum.ieee.org/tech-talk/computing/hardware/majorana-microsoft-backed-quantum-computer-research-retracted

Controversial Microsoft-backed research on elusive theoretical particles that could have proved a major advance in quantum computing has now been retracted after other scientists pointed out critical flaws in the work.

The original research focused on Majorana fermions, long-theorized particles that are their own antiparticles. First predicted more than 80 years ago by Italian physicist Ettore Majorana, scientists have yet to detect these self-annihilating particles inside particle accelerators.

However, in the past decade or so, researchers have detected signs of a kind of Majorana fermion known as a Majorana zero mode. This quasiparticle manifests in the form of groups of electrons and other particles collectively behaving as single particles.

In a 2018 study in Nature, Microsoft-backed scientists claimed they found strong evidence of these quasiparticles within a special kind of superconductor, a discovery they suggested could pave the way for a powerful kind of quantum computer. Now the researchers have officially retracted this work, citing "insufficient scientific rigor."

Majorana fermions could theoretically find use in the quantum bits, or qubits, at the heart of the most widely explored types of quantum computers. Whereas conventional computers switch transistors either on or off to symbolize data as ones and zeroes, because of the bizarre nature of quantum physics, qubits can exist in a state known as superposition where they can act as both 1 and 0. This essentially lets each qubit perform multiple calculations at once.

The more qubits are quantum-mechanically connected or entangled together, the more calculations they can simultaneously perform. Google and others have claimed evidence that their quantum computers have achieved a quantum advantage, outperforming even the most powerful modern supercomputers on certain tasks.

The quantum mechanical effects on which quantum computers depend – superposition and entanglement – are very fragile. However, Majorana zero modes could prove virtually immune to outside interference, a feature that Microsoft has suggested may help the company build a practical quantum computer.

The extraordinary resistance Majorana zero modes can have against disruption is rooted in topology, the branch of mathematics that investigates what aspects of shapes can survive deformation. When a pair of Majorana zero modes swap places – a technique similar to braiding two strands of hair – topology suggests these quasiparticles can in a sense remember how they behaved with respect to one another even after they get separated.

In theory, a "topological qubit" created from a pair of Majorana zero modes could benefit from a kind of protection conveyed by its topology. Even if one member of this duo runs into interference, the qubit can survive if its partner remains unscathed. This stability could help topological quantum computers scale up in power more easily than other approaches.

Directly proving that Majorana zero modes actually exist, however, has proven extraordinarily difficult. The 2018 work argued it discovered such evidence. However, these claims were "from the start implausible," says physicist Sergey Frolov at the University of Pittsburgh, whose investigations helped to trigger the Nature retraction.

In the 2018 study, researchers experimented with indium antimonide semiconductor nanowires covered with aluminum superconducting shells. In this hybrid material, a so-called "topological superconductor," previous research suggested Majorana particles should form at both ends of the wires.

When the scientists varied the voltage to their devices, they detected a sudden peak in their electrical conductance. They claimed this electrical signal was evidence of discrete, quantized levels of conductance, a hallmark of Majorana particles.

However, Frolov notes that when he and physicist Vincent Mourik at the University of New South Wales in Australia data from the 2018 work, they discovered major conflicts between the raw files and the published results. After their communication with the Microsoft-backed team proved fruitless, Frolov says, "we complained to Nature, Nature asked the authors for explanations, and then they retracted."

The retraction notes errors such as how the scientists "unnecessarily corrected" some of the data and mislabeled a graph. An independent review requested by the Delft University of Technology in the Netherlands suggests the researchers selected data that supported the phenomenon they were looking for while omitting conflicting data. However, this review found no evidence these errors were intentional. It further suggested the scientists were caught up in their enthusiasm and so did not pay enough attention to data that did not suit their purposes.

Although this research was retracted, some experts remain cautiously optimistic that the larger quest for topological qubits continues. "From the theoretical standpoint, there is no doubt that Majorana zero modes should exist in quantum wires and that, under appropriate conditions, they should give rise to quantized electrical conductance," says theoretical physicist Marcel Franz at the University of British Columbia in Vancouver, who co-wrote a commentary on the 2018 study. "The fact that no consensus has yet emerged on the experimental side, despite significant worldwide effort, is a testament to the enormous challenge that these experiments present to the physics community. I am optimistic however that in time, theory will be fully validated by experiments because, unlike in many other situations, we do understand the underlying mechanisms extremely well."

However, Frolov disagrees. He argues there is extensive theoretical work suggesting quantized conductance "to not be necessary for Majorana."

Microsoft says it continues to pursue topological quantum computing, and that its research does not rely on any of the claims or methods in the retracted work. "We are confident that scaled quantum computing will help address some of humanity's greatest challenges and we remain committed to the topological approach," says Zulfi Alam, head of the Microsoft Quantum team.

However, Frolov is skeptical that Majorana fermions may have any practical value. "In my opinion, topological qubits are a distant possibility, with or without this paper being valid," Frolov says. He notes that much like the Large Hadron Collider and LIGO, research into Majorana fermions is shedding light on fundamental physics, but suggests "it is a very long shot" that such work may have technological impacts.

"This will be more like CERN discovering a particle than like Thomas Edison inventing a lightbulb," he says.

16 Mar 2021

18 D-Wave demonstrates performance advantage in quantum simulation

by Maria Violaris

https://physicsworld.com/a/d-wave-demonstrates-performance-advantage-in-quantum-simulation/

Researchers at the quantum computing firm D-Wave Systems have shown that their quantum processor can simulate the behaviour of an "untwisting" quantum magnet much faster than a classical machine. Led

by D-Wave's director of performance research Andrew King, the team used the new low-noise quantum processor to show that the quantum speed-up increases for harder simulations. The result shows that even near-term quantum simulators could have a significant advantage over classical methods for practical problems such as designing new materials.

The D-Wave simulators are specialized quantum computers known as quantum annealers. To perform a simulation, the quantum bits, or qubits, in the annealer are initialized in a classical ground state and allowed to interact and evolve under conditions programmed to mimic a particular system. The final state of the qubits is then measured to reveal the desired information.

King explains that the quantum magnet they simulated experiences both quantum fluctuations (which lead to entanglement and tunnelling) and thermal fluctuations. These competing effects create exotic topological phase transitions in materials, which were the subject of the 2016 Nobel Prize in Physics.

The researchers used up to 1440 qubits to simulate their quantum magnet. In a study published in Nature Communications, they report that the quantum simulations were over three million times faster than the corresponding classical simulations based on quantum Monte Carlo algorithms.

Importantly, the experiment also showed that the speed of quantum simulations scaled better with the difficulty of the problem than the classical ones did. The quantum speed-up over classical methods was greater when the researchers simulated colder systems with larger quantum effects. The speed-up also increased when they simulated larger systems. Hence the quantum speed-ups are greatest for the hardest simulations, which can take classical algorithms extremely long times.

Advantage with a twist

The D-Wave team performed a similar quantum magnet simulation in 2018, but it was too fast to take accurate measurements of the system's dynamics. To slow down the simulation, the researchers added a so-called topological obstruction to the quantum magnet – essentially, a "twist" in the magnet that takes time to unravel. Together with a new low-noise quantum processor, this addition enabled them to accurately measure the system's dynamics.

"Topological obstructions can trap classical simulations that use quantum Monte Carlo algorithms, while a quantum annealer can circumvent the obstructions via tunnelling," explains Daniel Lidar, who directs the Center for Quantum Information Science and Technology at the University of Southern California, US, and was not involved with the research. "This work has demonstrated a speed-up arising from this phenomenon, which is the first such demonstration of its kind. The result is very interesting and shows that quantum annealing is promising as a quantum simulation tool."

In contrast with previous simulations comparing quantum and classical algorithms, King's experiment directly relates to a useful problem. Quantum magnets are already being investigated for their potential applications in creating new materials. Quantum speed-ups could rapidly accelerate this research; however, the D-Wave team does not rule out the possibility of developing faster classical algorithms than those currently used. The team ultimately sees the most promising upcoming applications of quantum simulations to be a hybrid of quantum and classical methods. "This is where we expect to find near-term value for customers," King says.

19 Quantum Computing and Reinforcement Learning Are Joining Forces to Make Faster AI

by Shelly Fan

https://singularityhub.com/2021/03/16/quantum-computing-and-reinforcement-learning-are-joining-forces-to-make-faster-ai/#:~:text=Quantum%20Computing%20and%20Reinforcement%20Learning%20Are%20Joining%20Forces%20to%20Make%20Faster%20AI,-By&text=Because%20the%20concept%20behind%20these,rewarded%20for%20its%20correct%20decisions.

Deep reinforcement learning is having a superstar moment.

Powering smarter robots. Simulating human neural networks. Trouncing physicians at medical diagnoses and crushing humanity's best gamers at Go and Atari. While far from achieving the flexible, quick thinking that comes naturally to humans, this powerful machine learning idea seems unstoppable as a harbinger of better thinking machines.

Except there's a massive roadblock: they take forever to run. Because the concept behind these algorithms is based on trial and error, a reinforcement learning AI "agent" only learns after being rewarded for its correct decisions. For complex problems, the time it takes an AI agent to try and fail to learn a solution can quickly become untenable.

But what if you could try multiple solutions at once?

This week, an international collaboration led by Dr. Philip Walther at the University of Vienna took the "classic" concept of reinforcement learning and gave it a quantum spin. They designed a hybrid AI that relies on both quantum and run-of-the-mill classic computing, and showed that – thanks to quantum quirkiness – it could simultaneously screen a handful of different ways to solve a problem.

The result is a reinforcement learning AI that learned over 60% faster than its non-quantum-enabled peers. This is one of the first tests that shows adding quantum computing can speed up the actual learning process of an AI agent, the authors explained.

Although only challenged with a "toy problem" in the study, the hybrid AI, once scaled, could impact real-world problems such as building an efficient quantum internet. The setup "could readily be integrated within future large-scale quantum communication networks," the authors wrote.

The Bottleneck

Learning from trial and error comes intuitively to our brains.

Say you're trying to navigate a new convoluted campground without a map. The goal is to get from the communal bathroom back to your campsite. Dead ends and confusing loops abound. We tackle the problem by deciding to turn either left or right at every branch in the road. One will get us closer to the goal; the other leads to a half hour of walking in circles. Eventually, our brain chemistry rewards correct decisions, so we gradually learn the correct route. (If you're wondering ... yeah, true story.)

Reinforcement learning AI agents operate in a similar trial-and-error way. As a problem becomes more complex, the number – and time – of each trial also skyrockets.

"Even in a moderately realistic environment, it may simply take too long to rationally respond to a given situation," explained study author Dr. Hans Briegel at the Universität Innsbruck in Austria, who previously led efforts to speed up AI decision-making using quantum mechanics. If there's pressure that allows "only a certain time for a response, an agent may then be unable to cope with the situation and to

learn at all," he wrote.

Many attempts have tried speeding up reinforcement learning. Giving the AI agent a short-term "memory." Tapping into neuromorphic computing, which better resembles the brain. In 2014, Briegel and colleagues showed that a "quantum brain" of sorts can help propel an AI agent's decision-making process after learning. But speeding up the learning process itself has eluded our best attempts.

The Hybrid AI

The new study went straight for that previously untenable jugular.

The team's key insight was to tap into the best of both worlds – quantum and classical computing. Rather than building an entire reinforcement learning system using quantum mechanics, they turned to a hybrid approach that could prove to be more practical. Here, the AI agent uses quantum weirdness as it's trying out new approaches – the "trial" in trial and error. The system then passes the baton to a classical computer to give the AI its reward – or not – based on its performance.

At the heart of the quantum "trial" process is a quirk called superposition. Stay with me. Our computers are powered by electrons, which can represent only two states – 0 or 1. Quantum mechanics is far weirder, in that photons (particles of light) can simultaneously be both 0 and 1, with a slightly different probability of "leaning towards" one or the other.

This noncommittal oddity is part of what makes quantum computing so powerful. Take our reinforcement learning example of navigating a new campsite. In our classic world, we – and our AI – need to decide between turning left or right at an intersection. In a quantum setup, however, the AI can (in a sense) turn left and right at the same time. So when searching for the correct path back to home base, the quantum system has a leg up in that it can simultaneously explore multiple routes, making it far faster than conventional, consecutive trail and error.

"As a consequence, an agent that can explore its environment in superposition will learn significantly faster than its classical counterpart," said Briegel.

It's not all theory. To test out their idea, the team turned to a programmable chip called a nanophotonic processor. Think of it as a CPU-like computer chip, but it processes particles of light – photons – rather than electricity. These light-powered chips have been a long time in the making. Back in 2017, for example, a team from MIT built a fully optical neural network into an optical chip to bolster deep learning.

The chips aren't all that exotic. Nanophotonic processors act kind of like our eyeglasses, which can carry out complex calculations that transform light that passes through them. In the glasses case, they let people see better. For a light-based computer chip, it allows computation. Rather than using electrical cables, the chips use "wave guides" to shuttle photons and perform calculations based on their interactions.

The "error" or "reward" part of the new hardware comes from a classical computer. The nanophotonic processor is coupled to a traditional computer, where the latter provides the quantum circuit with feedback – that is, whether to reward a solution or not. This setup, the team explains, allows them to more objectively judge any speed-ups in learning in real time.

In this way, a hybrid reinforcement learning agent alternates between quantum and classical computing, trying out ideas in wibbly-wobbly "multiverse" land while obtaining feedback in grounded, classic physics "normality."

A Quantum Boost

In simulations using 10,000 AI agents and actual experimental data from 165 trials, the hybrid approach,

when challenged with a more complex problem, showed a clear leg up.

The key word is "complex." The team found that if an AI agent has a high chance of figuring out the solution anyway – as for a simple problem – then classical computing works pretty well. The quantum advantage blossoms when the task becomes more complex or difficult, allowing quantum mechanics to fully flex its superposition muscles. For these problems, the hybrid AI was 63% faster at learning a solution compared to traditional reinforcement learning, decreasing its learning effort from 270 guesses to 100.

Now that scientists have shown a quantum boost for reinforcement learning speeds, the race for next-generation computing is even more lit. Photonics hardware required for long-range light-based communications is rapidly shrinking, while improving signal quality. The partial-quantum setup could "aid specifically in problems where frequent search is needed, for example, network routing problems" that's prevalent for a smooth-running internet, the authors wrote. With a quantum boost, reinforcement learning may be able to tackle far more complex problems – those in the real world – than currently possible.

20 Bangalore Scientists Discover New State Of Materials Useful To Create Controllable Quantum Technologies

https://swarajyamag.com/news-brief/bangalore-scientists-discover-new-state-of-materials-useful-to-create-controllable-quantum-technologies

Scientists have discovered a new exotic, strange state of materials in contact with an environment that alters its physical properties in the presence of an electromagnetic field, leading to better quantum technologies, which are tunable and controllable as per the user requirements.

Dibyendu Roy, Associate Professor, and his group from Raman Research Institute (RRI) Bangalore, an autonomous institute of the Department of Science and Technology, Government of India, have been exploring systems in contact with the environment or the open quantum systems and their physical properties for a while.

They explored ways to control the topological phase transitions of matter in contact with an environment by an external periodic perturbation such as laser light in their present work.

Topology is concerned with the properties of a geometric object preserved under continuous deformations, such as stretching and twisting.

Understanding various phases and phase transitions is of central importance in the study of matter. Generally, phase transitions are studied by assuming that the system is isolated, with little or negligible environmental interactions.

While studying the geometric phase in systems in contact with an environment and examining the environment's consequence on the band-structure topology of the systems, they discovered a new metallic state of the materials coupled to an environment, the Ministry of Science and Technology said in a statement.

They have shown that, in an external electromagnetic field, geometric properties of a crystalline solid with lattices arranged in a one-dimensional periodic manner can display phase transitions, thereby altering its physical properties.

This work funded by the Department of Science and Technology, India, via the Ramanujan Fellowship, and the Ministry of Electronics and Information Technology (MeitY), India, under a grant for"Centre for

Excellence in Quantum Technologies" has been published in the journal 'Physical Review B'.

In our everyday lives, several devices and technologies exploit some of the other aspects of quantum physics, like LEDs, semiconductor technology, and nanomaterials. Usually, the environmental interactions in such quantum systems are either neglected or are considered very small.

Through this work, the RRI team has shown that if such effects are carefully taken into account, one can drastically alter the quantum system's physical behavior and lead to better quantum technologies.

15 Mar 2021

21 At least 32 Indian companies have been attacked by cyber criminals using Microsoft's email servers

by IANS

https://www.businessinsider.in/tech/news/at-least-32-indian-companies-have-been-attacked-by-cyber-criminals-using-microsofts-email-servers/articleshow/81511936.cms

At least 32 Indian organisations have been attacked by hackers who exploited vulnerabilities in unpatched Microsoft business email servers, a new report warned on Monday, adding that the finance and banking institutions have been hit the most in the country.

The finance and banking institutions (28%) in India are followed by government-military organisations (16%), manufacturing (12.5%), insurance-legal (9.5%) and others (34%), according to Check Point Research.

Overall, the hacking attempts on organisations using the services of those unpatched on-premises servers have multiplied by more than six times (or tripled) in the past 72 hours.

The country most attacked was the US (21% of all exploit attempts), followed by The Netherlands (12%) and Turkey (12%), along with India.

Most targeted industry sector has been government-military (27% of all exploit attempts), followed by manufacturing (22%), and then software vendors (9%), the researchers noted.

"A full race has started among hackers and security professionals. Global experts are using massive preventative efforts to combat hackers who are working day-in and day-out to produce an exploit that can successfully leverage the remote code execution vulnerabilities in Microsoft Exchange," said the researchers from the cyber security firm.

Amid reports indicating that about five different hacking groups are attacking the business email servers of Microsoft, the tech giant has also detected a new family of ransomware.

Named as 'DearCry,' the new ransomware is "being used after an initial compromise of unpatched on-premises Exchange Servers," Microsoft said in a tweet last week. It uses the same four vulnerabilities that Microsoft linked to a new China-backed hacking group called "Hafnium".

On March 3, Microsoft released an emergency patch for its Exchange Server product, the most popular mail server worldwide. All incoming and outgoing emails, calendar invitations and virtually anything accessed within Outlook goes through the Exchange server.

Orange Tsai from DEVCORE, a security firm based in Taiwan, reported two vulnerabilities in January.

Unaware of the full magnitude of these findings, Microsoft was prompted to further investigate their Exchange server. The investigation uncovered five more critical vulnerabilities.

The vulnerabilities allow an attacker to read emails from an Exchange server without authentication or accessing an individual's email account.

Further vulnerability chaining enables attackers to completely take over the mail server itself.

"If your organisation's Microsoft Exchange server is exposed to the internet, and if it has not been updated with the latest patches, nor protected by a third party software, then you should assume the server is completely compromised," warned Lotem Finkelsteen, Manager of Threat Intelligence, Check Point Software.

Right now, the purpose of the attack and what cybercriminals wanted within the network is still unknown.

22 Traceability and end-to-end encryption cannot co-exist on digital messaging platforms

by aditi agrawal

https://www.forbesindia.com/article/take-one-big-story-of-the-day/traceability-and-endtoend-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which the government of India notified on February 25, were supposed to provide clarity on whether or not breaking end-to-end encryption is a limit that platforms must breach to enable traceability. Instead, even two weeks after the Rules have been notified, there is no clarity on what they mean for end-to-end encrypted messaging platforms.

Much of the debate around "enabling the identification of the first originator" or traceability on end-to-end encrypted platforms has circled around whether it is possible to identify the originator of a message without breaking or diluting end-to-end encryption. So much so that a crucial case on enabling traceability on WhatsApp, which got transferred to the Supreme Court from the Madras High Court, spent at least four hearings discussing whether or not traceability was possible without breaking end-to-end encryption. In the last hearing in January 2020, notification of these Rules was still awaited. The case is still pending.

The Indian government has maintained that it is indeed possible. However, WhatsApp, Signal, privacy advocates and other cryptography experts have vehemently said that enabling identification of the originator at the very least defeats the purpose of end-to-end encryption if not entirely breaks it.

The Indian government has thus far been proposing two schemes as potential solutions to the problem of identifying the originator: **Tagging each message** with the originator's information (as proposed by IIT Madras's Dr V Kamakoti); and **comparing hash values** of problematic messages with what WhatsApp/intermediary has (as discussed by Rakesh Maheshwari from the Ministry of Electronics and Information Technology [MeitY] at multiple public events).

Moxie Marlinspike, creator of the Signal protocol and CEO of Signal Messenger, told Forbes India a fortnight before the Rules were notified that "Signal is designed so that Signal does not know who is messaging who. Signal doesn't have that information." **On traceability, he said that end-to-end encryption and traceability cannot co-exist.** "There is no way to have data privacy for everybody

but just a specific set of people. [Once you make it possible] to just give the police access to data under some set of circumstances, anyone can get access to that data."

What is end-to-end encryption?

E2EE creates a secure, encrypted communication channel between two users that can never be intercepted. When, say, Alice and Bob communicate, both of them generate a public key and a private key. The former is visible to all others in the WhatsApp server and is necessary to start the communication. The private key is used to access their own messages and is known only to their devices. When Alice sends a "Hello" to Bob, it is encrypted in such a way that it can only be decrypted using a key which exists only on Alice and Bob's devices. And this unique key keeps changing with every message sent.

Signal Protocol, which is used by WhatsApp, Signal, and by Facebook Messenger and Skype for secret chats, is the most used end-to-end encryption protocol. Apple's iMessage is also an end-to-end encrypted messaging service but it uses a different protocol.

What is traceability?

The phrase "shall enable tracing out of such originator" in the draft amendments was replaced with "shall enable the identification of the first originator" in the notified Rules. According to the Information Technology Act, 2000, an originator is defined as "a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary".

The Kamakoti Solution: Tagging the message with originator's information

In May 2019, at the Madras High Court's directions, the then Chief Secretary of the Tamil Nadu government, Dr Girija Vaidyanathan, had convened a meeting between the Tamil Nadu police and social media intermediaries. It is at this meeting that Dr V Kamakoti, a computer science professor at IIT Madras and a member of the National Security Advisory Board (NSAB), had suggested that WhatsApp should consider including the phone number of the originator of the message every time it is forwarded.

This suggestion culminated in Kamakoti's official affidavit to the court, which has shaped much of the debate around traceability in India. In fact, language similar to what Kamakoti has used in the affidavit, where emphasis has been laid on not decrypting the content of the message itself, has found itself space in the Rules as a proviso.

Kamakoti proposed two levels of encryption. The message "Hello" remains encrypted as it is now, while the originator's information gets tagged along with the "Hello" in an encrypted manner every time the message is forwarded. The decryption key to the originator information, in this schema, is retained in an escrow with WhatsApp (think Blackberry's encryption model). Once a problematic message is reported to a law enforcement agency, the latter goes to WhatsApp with the message and WhatsApp uses its key to decrypt the originator's information. The decryption can happen only if relevant court orders are produced by the law enforcement agencies.

In an interview with MediaNama in 2019, Kamakoti had explained that there are two things to consider – tagging messages as forwardable or not-forwardable, and who is the originator. For the former, he said that the originator of the message should have the option of marking each message as "forwardable" or

"not forwardable" as a method of giving consent. In the former case, the originator assumes responsibility for the message and their originator information gets attached to the message. If a recipient forwards/sends a "not forwardable" message, the recipient then becomes the originator.

It is only in the case of simple forwards that the originator information travels along with the message. If a recipient copy pastes the text, they essentially change it and become the originator. If the recipient takes a screenshot and sends it, they become the originator. In case of a media file, if a recipient adds a comment to it, they become the originator, as per Kamakoti's proposal.

Kamakoti's proposal was decried by WhatsApp, cryptographic experts and advocates of privacy and free speech. In its response to the court, WhatsApp had submitted that Kamakoti's proposal would "wholly undermine its [WhatsApp's] end-to-end encryption as users would be afraid to freely express themselves if their private thoughts would forever be linked to their identities".

Problems included falsely labelling someone as the originator even though they found that content on other platforms or elsewhere and copied it from there. This is a problem that Google, too, had highlighted during the proceedings in Madras High Court – the counsel for Google had said that even for YouTube, finding the originator was difficult as the originator of the content is not necessarily the first person who created the content itself, and potentially on another platform.

WhatsApp had also submitted that in the attempt to get to the originator, innocent people may get caught as savvier criminals would use modified versions of the app to potentially frame others. Modified versions of apps are very common wherein they are sideloaded (downloaded from the internet directly onto phones without being mediated through official app stores) and features are cherry-picked as per the user's convenience. It is practically impossible for all official developers, not just WhatsApp, to shut down every such modified app.

WhatsApp had also said that often forwarded messages do not give the context that may have accompanied the original message, thereby skewing the intent and meaning of the message itself.

A bigger problem is that storing a master key for the originator information makes WhatsApp a prime target for hackers and defeats the purpose of data minimisation.Forbes India has a copy of WhatsApp's submission.

Digital rights organisation, the Internet Freedom Foundation, which is an intervener in the traceability case, too had submitted a technical affidavit against Kamakoti's proposal. Authored by IIT Bombay's Dr Manoj Prabhakaran, a computer science professor who specialises in cryptography, the affidavit said that not only did traceability erode all users' privacy, it also was not an effective means of fighting fake news. He had warned that adding a digital signature to every message would have a "chilling effect on the right to free speech". He had instead proposed a feature that could allow users to anonymously send viral messages to a server and make them publicly available.

All proponents of end-to-end encryption have argued that traceability undermines the right to communicate anonymously on the internet, a feature that makes it easier for human rights activists, dissenters, people belonging to vulnerable and marginalised groups to be targeted by authoritarian states, malicious actors, and those in power.

In an interview with Forbes India before the Rules were notified, in response to a question about the feasibility of Kamakoti's solution, Signal's Marlinspike had said, "Anytime someone says something about escrow that just means that it is unencrypted. It is the same situation where you either have one or you don't. Signal has been meticulously designed to keep your data in your hands instead of ours." He mentioned how there are two ways of looking at security – computer security which is a "losing strategy for the last

30 years", and information security wherein "information itself is encrypted". The latter means that if they are stored on computers and computers cannot be secured, it does not matter as the information itself is secure.

"I don't think Prof. Kamakoti's suggestion as stated is currently feasible. This is very definitional. When cryptographers say end-to-end encryption, we mean a very particular thing where to anyone except the sender and the receiver, messages should look like garbage, and an outsider should not be able to tell [beyond just traffic analysis] which message was sent to whom," Dr Debayan Gupta, an assistant professor of computer science at Ashoka University, tells Forbes India.

Gupta warns that the moment there is something that is sent along every message which can be tracked by WhatsApp, the definition of end-to-end encryption breaks. "In an ideal end-to-end encrypted scenario, if there are two messages that I can send to you, WhatsApp should not be able to know which message I sent to you," he says.

Tracing the originator through a catalogue of hashes

At an online event organised by the Internet Society and the CCAOI after the Rules were notified, Rakesh Maheshwari, the group coordinator for cyber laws at MeitY, proposed another solution. The idea is that when a user approaches a law enforcement agency with a problematic message, the law enforcement agency can go to WhatsApp and ask the platform to search for the hash in a catalogue of hashes to find the originator. Maheshwari's assumption is that forwarded messages whose content does not change would have the same hash.

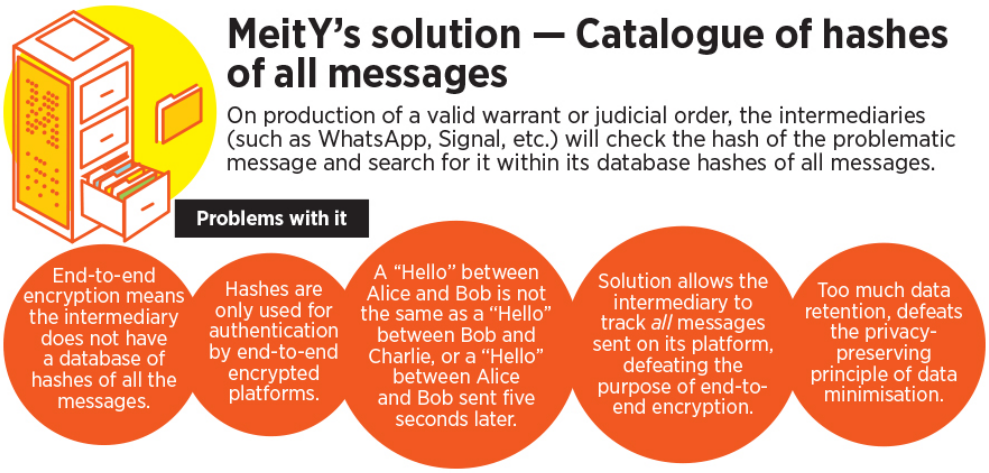
Hashing is a mathematical function through which the integrity of data is ascertained. For instance, if I write "hello" and run a hashing function on it, it may be hashed as A$F. The slightest change in the input data – "HEllo" instead of "hello" – would result in a change in hash. This technique is also used in digital forensics to ensure that digital evidence, such as a hard drive, has not been tampered with. When a hard drive is seized, it is immediately hashed and the hashes are shared with both the prosecution and

the defence. At a later date, if either side wants to confirm the integrity of the hard drive in question, they hash the hard drive again. A change in a single character of the hash would mean that the hard drive has been tampered with.

Gupta warns that the solution proposed by Maheshwari is not feasible. That is because when a hash is generated for a message in an end-to-end encrypted platform, it takes into account the unique identity keys of that particular sender and receiver in addition to the encrypted message itself.

This means, the hash value of a "Hello" that Alice sends to Bob is different from the hash value of "Hello" that Bob sends/forwards to Charlie. If Charlie were to go to the police with the "Hello" that Bob sent to him, even if WhatsApp could search for the hash generated, it would only lead to one message – the one between Bob and Charlie. Alice will not turn up. The only way WhatsApp could make Alice turn up is if it breaks its "double ratcheting" algorithm that changes the key between two users for every message in a feature that is called "forward secrecy". Moreover, because Alice and Bob's keys keep changing with every message, even if Alice were to send Bob "Hello" twice, both will have different hashes.

Gupta warns that this means WhatsApp will be able to track all the messages that people send on its platform, thereby defeating the entire purpose of end-to-end encryption. Furthermore, this means that WhatsApp will retain entirely too much (meta) data, thereby defeating the privacy-preserving principle of data minimisation.



OTR deniability means you can't get to the originator

Signal Protocol, which is the one that WhatsApp uses to implement end-to-end encryption, also offers off-the-record deniability, better known as OTR deniability. When Alice sends Bob a message "Hello", Alice locks the message in a box (let's call this "encryption") with a key, which is unique to this particular message between Alice and Bob which no one else knows, and Alice signs the outside of the box. To anyone else who tries to get to the message (interception), they will only see a random string of characters because of the encryption at play. Bob, who is the only one who has a copy of that unique key, on receiving the box (encrypted message), is sure that it has come from Alice. But, later on, Bob cannot prove to anyone else that Alice sent that particular message: Because the signing key was derived from a value shared by Bob. Once Bob receives the message, he also has the ability to change/forge it himself if he has enough technical know-how.

Gupta explains that such technical know-how is quite common. “Many of my undergraduates can do these things,” he says. Once messages are decrypted, they are stored in the local databases of the smartphone where they can be accessed by rooting the device. Think of it as getting admin access to your smartphone. Then, Bob can change the message “Hello” from Alice to “Hello, you are a buffalo” because he has access to that unique key.

Gupta explains that the user need not have the technical ability themselves either. That is because there are multiple variants of WhatsApp that are available for people to sideload. These copies still use the Signal Protocol because of which they can still use the E2EE offered by WhatsApp, but they pick and choose the other features of the app client itself.

Other solutions like digital signatures have limitations

A cryptographic expert who spoke to Forbes India on the condition of anonymity said that originator tracing might not be the best way to thwart malicious viral messages. “But if that is the path one chooses, then a reasonable way to implement it without affecting much else – including end-to-end encryption – is to require a digital signature of an Indian originator to be attached to any message intended for a large audience,” he says. If a message is sent to a group without this signature, it will not be shown to the recipients; it could be shown in on-to-one messaging but would not be forwardable. This is a slightly more refined version of what Kamakoti had proposed.

“While international (or reverse-engineered) versions of the app can originate a message without attaching a signature, they will not be forwarded further by the legitimate Indian installations of the app, thereby preventing them from going viral in India,” he further explains. Indian users would be able to forward an unsigned message by explicitly choosing to become the originator, maybe through a pop-up informing them about the Rules and them becoming the originator and thus liable for the message.

Here, the expert warns that the digital signatures must also be end-to-end encrypted so that WhatsApp servers cannot distinguish between signed and unsigned messages. “When a viral message is caught in the wild with a signature, the authorities can collaborate with WhatsApp to trace the signer of the message to a WhatsApp account. The cryptographic security of digital signatures would guarantee that the message was indeed endorsed by the identified WhatsApp account, unless their device was compromised. However, an individual may still be framed if their identity was used to acquire the phone number registered with WhatsApp,” he adds.

Having said this, the expert also warns that this move would have a massive chilling effect on free speech, “disproportionate to the goal of tracing the source of viral messages”. Also, digital signatures must be allowed to expire. Without such expiration date, “old messages can be revived several years down the line, in a different context”. “Secondly, to be able to trace the originator in such a case, WhatsApp will have to retain all the public keys all the (Indian) users ever used, forever. This would be problematic as keys need to be frequently renewed for security and privacy purposes,” experts say.

Does it solve the problem?

Both Gupta and the anonymous expert concurred that traceability barely solves the problem of getting to people who systematically spread malicious information. Instead, it would keep netting less digitally savvy folks for not being media literate enough.

One of the biggest issues, of course, is how do you establish beyond doubt that the first originator is indeed the first person within the physical territory of India to send the message. What happens if people

use VoIP [Voice over Internet Protocol] numbers and VPNs [Virtual Private Networks] through which they neither have a +91 number, nor an Indian IP address connected to their user account? What if someone with a +91 number immigrates to the US and retains their old WhatsApp or Signal account? Would they be held responsible? Beyond VPNs, it is very easy to spoof IP addresses and location data. "Children were doing this when they were attempting to catch Pokémon," Gupta jokes. Gupta also warns that the Rules don't take into account the global nature of communication over internet-based apps. If there are two versions of WhatsApp – one for India and one for the rest of the world – , "it is not clear how you would change that protocol at the edges of this geographical entity called India". "How would that cross-protocol communication happen?" Gupta asks. He reminds that "the Internet is not a sovereign territory" to which "territorial sovereign laws" can be easily applied. "The originator of the information bit needs to be cleared up very carefully," he says.

Even if WhatsApp and Signal were to somehow introduce traceability, the actual criminals would move to other platforms that have not attracted similar kind of regulatory scrutiny. It is important to remember that the traceability rule only applies to significant social media intermediaries, that is, only platforms that have more than 50 lakh users. If petty criminals, members of organised crime, and professional propagators of misinformation move to smaller apps, they are as it is not covered by the Rules.

"Before we break this beautiful protocol and technology and build patches for it, we as cryptographers want to make sure we understand what the requirements are," says Gupta, adding that this discussion should have happened before the Rules were notified, not after.

23 Nanophotonics Could Be the 'Dark Horse' of the Quantum Computing Race, New Paper Says

by Edd Gent

https://singularityhub.com/2021/03/15/nanophotonics-could-be-the-dark-horse-of-the-quantum-computing-race-new-paper-says/

The race to build the first practical quantum computers looks like a two-horse contest between machines built from superconducting qubits and those that use trapped ions. But new research suggests a third contender – machines based on optical technology – could sneak up on the inside.

The most advanced quantum computers today are the ones built by Google and IBM, which rely on superconducting circuits to generate the qubits that form the basis of quantum calculations. They are now able to string together tens of qubits, and while controversial, Google claims its machines have achieved quantum supremacy – the ability to carry out a computation beyond normal computers.

Recently this approach has been challenged by a wave of companies looking to use trapped ion qubits, which are more stable and less error-prone than superconducting ones. While these devices are less developed, engineering giant Honeywell has already released a machine with 10 qubits, which it says is more powerful than a machine made of a greater number of superconducting qubits.

But despite this progress, both of these approaches have some major drawbacks. They require specialized fabrication methods, incredibly precise control mechanisms, and they need to be cooled to close to absolute zero to protect the qubits from any outside interference.

That's why researchers at Canadian quantum computing hardware and software startup Xanadu are backing an alternative quantum computing approach based on optics, which was long discounted as

impractical. In a paper published last week in Nature, they unveiled the first fully programmable and scalable optical chip that can run quantum algorithms. Not only does the system run at room temperature, but the company says it could scale to millions of qubits.

The idea isn't exactly new. As Chris Lee notes in Ars Technica, people have been experimenting with optical approaches to quantum computing for decades, because encoding information in photons' quantum states and manipulating those states is relatively easy. The biggest problem was that optical circuits were very large and not readily programmable, which meant you had to build a new computer for every new problem you wanted to solve.

That started to change thanks to the growing maturity of photonic integrated circuits. While early experiments with optical computing involved complex table-top arrangements of lasers, lenses, and detectors, today it's possible to buy silicon chips not dissimilar to electronic ones that feature hundreds of tiny optical components.

In recent years, the reliability and performance of these devices has improved dramatically, and they're now regularly used by the telecommunications industry. Some companies believe they could be the future of artificial intelligence too.

This allowed the Xanadu researchers to design a silicon chip that implements a complex optical network made up of beam splitters, waveguides, and devices called interferometers that cause light sources to interact with each other.

The chip can generate and manipulate up to eight qubits, but unlike conventional qubits, which can simultaneously be in two states, these qubits can be in any configuration of three states, which means they can carry more information.

Once the light has traveled through the network, it is then fed out to cutting-edge photon-counting detectors that provide the result. This is one of the potential limitations of the system, because currently these detectors need to be cryogenically cooled, although the rest of the chip does not.

But most importantly, the chip is easily re-programmable, which allows it to tackle a variety of problems. The computation can be controlled by adjusting the settings of these interferometers, but the researchers have also developed a software platform that hides the physical complexity from users and allows them to program it using fairly conventional code.

The company announced that its chips were available on the cloud in September of 2020, but the Nature paper is the first peer-reviewed test of their system. The researchers verified that the computations being done were genuinely quantum mechanical in nature, but they also implemented two more practical algorithms: one for simulating molecules and the other for judging how similar two graphs are, which has applications in a variety of pattern recognition problems.

In an accompanying opinion piece, Ulrik Andersen from the Technical University of Denmark says the quality of the qubits needs to be improved considerably and photon losses reduced if the technology is ever to scale to practical problems. But, he says, this breakthrough suggests optical approaches "could turn out to be the dark horse of quantum computing."

14 Mar 2021

24 Clever Method to Protect Satellite Communications from Quantum Computing

https://qubitreport.com/quantum-computing-cybersecurity-and-cryptography/2021/03/14/clever-method-to-protect-satellite-communications-from-quantum-computing/

Securing communications is on the forefront of anyone involved in the cybersecurity industry. With the looming advent of quantum computing's threat to encryption, there is reason to race towards a solution. One such avenue is a method descriptively titled "**Symbol Waveform Hopping**", or **SWH**.

The SWH method is in development by the Astrapi Corporation, under contract to the U.S. Air Force. Utilizing new techniques in mathematical applications, Astrapi's method enables transmission security in satellite communications.

> "We are quite encouraged and excited about this advanced approach to securing communication transmission. Symbol Waveform Hopping has broad application across multiple sectors. This technology represents a major derivative advancement of our Spiral Modulation capability. We are making foundational improvements right at the core physical layer of the communications stack ... It complements other very powerful and innovative developments by Astrapi," said Dr. Jerrold Prothero, Founder and CEO of Astrapi Corporation.

The Crux

Encoding of satellite transmissions using frequency hopping, or FH, is a well-established process. Basic telecommunications take Euler's equation to the application of four fundamentals of telecommunication signals:

- Error rate
- Bandwidth
- Strength
- Throughput

Redesigning the symbol waveforms in fundamentally new ways is the crux of the methodology, with Euler's formula still in play. The difference from the FH method is SWH's use of time vice frequency in transmission execution.

The Benefits

SWH is does not require encryption of the transmission. In forfeiting this requirement, SWH does not require processing cycles to encrypt or decrypt data. This savings in processing to achieve secure transmission (theoretically) also precludes the need for power, a staple for all electronics, and a premium commodity for satellite operation.

The Security

SWH is protected by physics by presenting images smaller than the noise floor. Ergo, an intercepted signal should not be resolvable as it is below the threshold of recognizability by the underlying receiver.

Without the need for highly complex encryption algorithms to secure the data, high overhead processing costs and power consumption are not needed. In this security solution, there is no readily-apparent target for quantum computing. This is the security strength SWH theoretically holds over quantum computing.

25 White House Weighs New Cybersecurity Approach After Failure to Detect Hacks

by David E. Sanger, Julian E. Barnes & Nicole Perlroth

https://www.nytimes.com/2021/03/14/us/politics/us-hacks-china-russia.html

The sophisticated hacks pulled off by Russia and China against a broad array of government and industrial targets in the United States – and the failure of the intelligence agencies to detect them – are driving the Biden administration and Congress to rethink how the nation should protect itself from growing cyberthreats.

Both hacks exploited the same gaping vulnerability in the existing system: They were launched from inside the United States – on servers run by Amazon, GoDaddy and smaller domestic providers – putting them out of reach of the early warning system run by the National Security Agency.

The agency, like the C.I.A. and other American intelligence agencies, is prohibited by law from conducting surveillance inside the United States, to protect the privacy of American citizens.

But the F.B.I. and Department of Homeland Security – the two agencies that can legally operate inside the United States – were also blind to what happened, raising additional concerns about the nation's capacity to defend itself from both rival governments and nonstate attackers like criminal and terrorist groups.

In the end, the hacks were detected long after they had begun not by any government agency but by private computer security firms.

The full extent of the damage to American interests from the hacks is not yet clear, but the latest, attributed by Microsoft to China, is now revealing a second vulnerability. As Microsoft releases new "patches" to close the holes in its system, that code is being reverse-engineered by criminal groups and exploited to launch rapid ransomware attacks on corporations, industry executives said. So a race is on – between Microsoft's efforts to seal up systems, and criminal efforts to get inside those networks before the patches are applied.

"When not one but two cyberhacks have gone undetected by the federal government in such a short period of time, it's hard to say that we don't have a problem," said Representative Mike Gallagher, Republican of Wisconsin and a co-chairman of a congressionally mandated cyberspace commission. "The system is blinking red."

The failures have prompted the White House to begin assessing options for overhauling the nation's cyberdefenses even as the government investigates the hacks. Some former officials believe the hacks show Congress needs to give the government additional powers.

But briefing reporters on Friday about the progress of the investigations, senior administration officials

said the White House had no plans to urge Congress to rewrite the laws that prevent American intelligence agencies from operating inside America's borders.

One senior adviser to President Biden said, however, that a new structure was needed, one that combined traditional intelligence collection with the talents of private-sector firms.

It was FireEye, a cybersecurity company, that ultimately found the SolarWinds attack organized by Russia, and a small Virginia firm named Volexity that revealed to Microsoft the fact that Chinese hackers found four previously unknown vulnerabilities in their systems, exposing hundreds of thousands of computer servers that use Microsoft Exchange software.

But even as officials try to assemble the lessons of those attacks, the one on Microsoft's systems, used by companies and government agencies, has grown more complex. On Friday, Microsoft warned that cybercriminals are using the back doors Chinese hackers left behind to deploy ransomware, which is used to lock up computer systems until payment is made.

The first efforts to freeze up American systems began Thursday night, Microsoft said, and American officials warned Friday that its customers had limited time, "measured in hours, not days" to patch their systems to avoid a costly nightmare.

Mr. Biden was briefed last week on the effort to seal up the holes in federal defenses, a senior administration official told reporters on Friday, adding that the federal government was in the third week of a monthlong effort to plug holes made obvious by the SolarWinds hack. A presidential order on longer-range fixes is coming.

But the first problem is detecting attacks – and there the United States has enormous work to do.

America's foremost hacking teams and digital defenders reside in Fort Meade, Md., home to the National Security Agency and its military counterpart, United States Cyber Command. Over more than a decade, with billions of dollars in new technology, they have littered foreign networks with various forms of "beacons" that give them access to detect attacks as they are coming together or begin.

But, like missile defense, that is hardly an impermeable shield. And foreign actors have begun to identify America's blind spot: If hackers can assemble an attack from inside America's borders, the U.S. government's best hunt-teams can be blindsided.

"The N.S.A. cannot operate in the domestic infrastructure," retired Adm. Michael S. Rogers, the former director of the agency, said on Friday at the Kellogg School of Management at Northwestern University. "You can't defend something you can't see."

But there is no political appetite to reverse decades of limits on intelligence agencies to monitor and defend network traffic inside the United States.

Instead, Biden administration officials said they would seek a deeper partnership with the private sector, tapping the knowledge of emerging hacking threats gathered by technology companies and cybersecurity firms.

The hope, current and former officials say, is to set up a real-time threat sharing arrangement, whereby private companies would send threat data to a central repository where the government could pair it with intelligence from the National Security Agency, the C.I.A. and other spy shops, to provide a far earlier warning than is possible today.

"You could stop attacks dead in their tracks," said Glenn S. Gerstell, a former general counsel for the National Security Agency. "We need a way to get threat intelligence into a one-stop shopping center."

The question is how to set up such a system.

After revelations in 2013 by the former intelligence contractor Edward J. Snowden that set off a debate about government surveillance, American technology companies are wary of the appearance of sharing data with American intelligence agencies, even if that data is just warnings about malware. Google was stung by the revelation in the Snowden documents that the National Security Agency was intercepting data transmitted between its servers overseas. Several years later, under pressure from its employees, it ended its participation in Project Maven, a Pentagon effort to use artificial intelligence to make its drones more accurate.

Amazon, in contrast, has no such compunctions about sensitive government work: It runs the cloud server operations for the C.I.A. But when the Senate Intelligence Committee asked company officials to testify last month – alongside executives of FireEye, Microsoft and SolarWinds – about how the Russians exploited systems on American soil to launch their attacks, they declined to attend.

Companies say that before they share reporting on vulnerabilities, they would need strong legal liability protections.

The most politically palatable headquarters for such a clearinghouse – avoiding the legal and civil liberties concerns of using the National Security Agency – would be the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. Mr. Gerstell described the idea as "automated computer sensors and artificial intelligence acting on information as it comes in and instantaneously spitting it back out."

The department's existing "Einstein" system, which is supposed to monitor intrusions and potential attacks on federal agencies, never saw the Russian attack underway – even though it hit nine federal departments and agencies. The F.B.I., lawmakers say, does not have broad monitoring capabilities, and its focus is divided across other forms of crime, counterterrorism and now domestic extremism threats.

"I don't want the intelligence agencies spying on Americans, but that leaves the F.B.I. as the de facto domestic intelligence agency to deal with these kinds of attacks," said Senator Angus King, a Maine independent, member of the Senate Intelligence Committee and co-chairman of the cyberspace commission. "I'm just not sure they're set up for this."

There are other hurdles. The process of getting a search warrant is too cumbersome for tracking nation-state cyberattacks, Mr. Gerstell said. "Someone's got to be able to take that information from the N.S.A. and instantly go take a look at that computer," he said. "But the F.B.I. needs a warrant to do that, and that takes time by which point the adversary has escaped."

Another obstacle is the slowness of identifying attackers. While the director of national intelligence concluded that the SolarWinds attack, carried out last year, was "likely" Russian in origin, a definitive assessment is not expected until this week or next. Only then can the United States respond with sanctions or cyberoperations – nearly a year after the attack began.

"The thing that worries me in both of these cases, too, is just how slowly we tend to attribute, and respond," Mr. Gallagher said.

On Friday, Jake Sullivan, the president's national security adviser, told reporters that an investigation was underway to identify who was behind using the hack of the Microsoft systems to spy on law firms, infectious disease research, universities, military contractors, think tanks and other targets. Microsoft has already said the hackers were a Chinese, state-backed group.

Last month, in the days before Microsoft released an emergency patch for vulnerable Exchange Servers,

multiple state-backed Chinese groups were apparently tipped off that the company was testing a patch. They began gorging on vulnerable systems with a speed and aggression that some security experts said they had never seen before.

It is unclear how exactly these Chinese groups learned of Microsoft's patch, but the timing suggests they caught wind of the moves when Microsoft rolled out a test version of its patch to its security partners at cybersecurity firms in late February.

Eighty companies participate in a longstanding partnership with Microsoft, known as the Microsoft Active Protections Program, including 10 Chinese firms. Microsoft confidentially alerts these companies to emerging cyberthreats and vulnerabilities ahead of its official patch cycle. The company is investigating whether one of its partners may have leaked to Chinese hackers or was itself hacked.

Microsoft said that if it determined a leak was responsible for the spike in attacks, the responsible partners would "face consequences."

The attacks forced Microsoft to release its patch one week early, on March 2. Within a week, the number of vulnerable Exchange servers dropped from 400,000 to 100,000, according to RiskIQ, an internet security company.

Now, however, 82,000 servers are still awaiting updates. Among those still vulnerable are more than 400 state, local and federal government entities in the United States – including more than a dozen servers run by federal agencies – according to an analysis by BitSight, a cybersecurity risk ratings company. The Biden administration has said nothing about the scope of federal vulnerability.

If the government is able to attribute the Microsoft attack to the Chinese, Mr. Gallagher said, there are "a variety of things we could do to inflict pain" on the government in Beijing.

26 US designates five Chinese companies as security threats

https://www.wionews.com/world/us-designates-five-chinese-companies-as-security-threats-370412

In light of the worsening relations between the United States and China, Washington has labeled Chinese tech companies, including Huawei, as national security threats.

"The (US) Federal Communications Commission's Public Safety and Homeland Security Bureau today released a list of communications equipment and services that have been deemed a threat to national security ... The list includes five Chinese companies that produce telecommunications equipment and services that have been found to pose an unacceptable risk to US national security or the security and safety of US persons," the FCC said in a statement on Friday.

President Joe Biden may be continuing his predecessor's hardline stance against China's growing technological dominance. The companies include Chinese telecommunications giant **Huawei**, along with **ZTE**, **Hytera Communications**, **Hangzhou Hikvision Digital Technology** and **Dahua Technology**.

"This list is a big step toward renewing trust in our communications networks Americans are relying on our networks more than ever to work, go to school, or access healthcare, and we need to trust that these communications are safe and secure," FCC Acting Chairwoman Jessica Rosenworcel said in a statement.

"This list provides meaningful guidance that will ensure that as next-generation networks are built across the country, they do not repeat the mistakes of the past or use equipment or services that will pose

a threat to US national security or the security and safety of Americans," she added.

According to South China Morning Post (SCMP), the designation came atop a number of moves Washington made against Huawei during the Trump administration, including banning US firms from using the company's technology to build wireless networks and placing the company on an entity list that prevents it from procuring US technology without government approval.

12 Mar 2021

27 The future of data privacy: confidential computing, quantum safe cryptography take center stage

by Charlie Osborne

https://www.zdnet.com/article/the-future-of-tech-confidential-computing-quantum-safe-cryptography-take-center-stage/

Confidential computing, quantum safe cryptography, and fully homomorphic encryption are set to change the future of data privacy as they make their way from a hypothesis to viable commercial applications.

On Thursday, IBM Research hosted an online program exploring each of these technologies and how they could impact how we securely manage, encrypt, store, and transfer information – with each solving a different challenge posed by future data privacy concerns.

confidential computing

IBM has been working on confidential computing for roughly a decade. The concept behind the technology is to permit clients to retain full privacy and control over data and operational workloads through hardware-level security.

This can include the implementation of "secure enclaves" – trusted execution environments – which can manage data and are only accessible through authorized programming code, keeping information away not only from cloud or infrastructure providers but also external threat actors.

IBM likens the technology to a hotel room safe, in which keycards are required to access the room, but further authorization is required to open the lock to the safe.

According to Hillery Hunter, VP and CTO at IBM Cloud, initial commercial applications of this technology are already embedded in financial services, telecoms, and healthcare offerings. Clients include Daimler and Apple for the CareKit SDK.

In November, IBM and AMD announced a collaborative partnership to work on confidential computing and hybrid cloud deployments.

Google Cloud, too, is investigating the technologies through virtual machines (VMs) which utilize confidential computing principles to secure data both at rest and in transit, and Intel's third-generation Xeon Ice Lake chips have been developed in order to handle the processor demands of confidential computing.

quantum safe cryptography & standardization

Quantum safe cryptography aims to tackle the problems that will arrive with the day we have a working quantum machine.

While quantum computing is being actively worked on by engineers worldwide, with Honeywell, for example, ramping up the capacity of its own System Model H1 to a quantum volume of 512, it is estimated that a full-capacity quantum computer could exist within the next 10 to 15 years.

When that day arrives, however, the high computational power of these machines would render "virtually all electronic communication insecure," according to IBM, as quantum computers are able to factor large numbers – a core precept of today's cryptography.

To resolve this, standards based on lattice cryptography have been proposed. This hides data in complex algebraic structures and is considered to be an attractive option for future-proofing data privacy architectures.

According to IBM cryptographer Vadim Lyubashevsky, adopting lattice frameworks is unlikely to impact end-users – and may actually improve computational performance.

But why bother now, when full quantum machines do not exist? According to mathematician Dustin Moody from the National Institute of Standards and Technology (NIST), the enterprise should look at adopting lattice, "quantum safe" cryptography as soon as it is commercially viable to do so.

Moody says that large-scale quantum computers could be used in attacks able to break cryptography used today – and so, all an attacker needs to do is harvest information now and store it for decryption in the future.

"It's important to make sure we can counter this threat now," Moody added. "There will be a transition with these algorithms, and it won't necessarily be easy. We are trying to prepare as much as we can and encourage others to do so."

To this end, NIST has launched the post-quantum cryptography project (PQC), which has elicited proposed algorithms for post-quantum encryption. At present, seven applications are under review and a standard is expected to be selected between 2022 and 2023.

fully homomorphic encryption

Fully homomorphic encryption (FHE) is sought after as a "Holy Grail" of encryption. FHE is a form of encryption that allows information to remain encrypted during computation and processing, regardless of the infrastructure or cloud technologies managing the data.

For example, data could be transferred between different parties and the cloud, analyzed, and sent back without ever being viewed or being made available in plaintext.

FHE utilizes different mathematical algorithms to the encryption we use today and has been in development over the past decade.

While FHE could be transformational in the data privacy arena, the issue is the vast processing power and time is required to facilitate encrypted data processing – especially when it comes to large datasets used by the enterprise or in research.

Scientists are working on ways to improve the efficiency of FHE algorithms and due to their efforts – as well as the development of hardware able to support FHE – early-stage use cases are now being explored.

Enterprise firms are under pressure from increasing data protection regulations and the risk of penalties and fines if data is not adequately protected. At the same time, however, they also need to capitalize on

data to create competitive differentiators and improve their operations, as well as to explore new business opportunities.

According to Eric Maass, Director of Strategy & Emerging Technology at IBM, the challenge is "extracting the value of the data while preserving its privacy."

In December, the firm launched the IBM Security Homomorphic Encryption Services, a platform designed to allow the enterprise to experiment with FHE in tandem with existing IT architecture, products, and data.

Intel is working with the US Defense Advanced Research Projects Agency (DARPA) on the Data Protection in Virtual Environments (DPRIVE) program, designed to bring down the cost and time of FHE implementations, and companies including Microsoft, Duality Technologies, Galois, and SRI International are also working toward the same goal.

Maass believes that highly-regulated industries, such as healthcare or financial organizations, will be "early adopters in this space."

28 New Approach To Sending & Receiving Information With Single Photons of Light Could Lead To "Land Beyond Silicon", Says University of Michigan Research Team

by James Dargan

https://thequantumdaily.com/2021/03/12/new-approach-to-sending-receiving-information-with-single-photons-of-light-could-lead-to-land-beyond-silicon-says-university-of-mic
#:~:text=New%20Approach%20To%20Sending%20%26%20Receiving,University%20of%20Michigan%20Research%20Team&text=A%20password%20will%20be%20e%2Dmailed%20to%20you.

Nonlinearity

A new discovery led by the University of Michigan (UM) could ultimately lead to the ability to send and receive information with single photons of light.

The research paper, entitled the tongue-twistingly Van der Waals heterostructure polaritons with moiré-induced nonlinearity, was published in the scientific journal Nature this month and is based on an international team of scientists' work.

The researchers were able to demonstrate that by using a phenomenon called "nonlinearity" to change and identify very weak light signals, they could utilize the changes into a quantum system which could give rise to better, more efficient computers in the future.

This approach can ultimately assist silicon-electronics-based information technology as heating and energy consumption considerations compromise it.

And because of it, nonlinear optics is viewed by many as a potential solution.

Quantum Egg Carton

The quantum "egg carton", as it is known, catches and releases photons, which gives it extra energy. This is conducive to quantum states because as the energy in the system increases, it requires more energy to get it to the nonlinearity of the next excited state.

"Researchers have wondered whether detectable nonlinear effects can be sustained at extremely low power levels – down to individual photons. This would bring us to the fundamental lower limit of power consumption in information processing," said Hui Deng, professor of physics at the University of Michigan and senior author of the paper.

While also adding: "We demonstrated a new type of hybrid state to bring us to that regime, linking light and matter through an array of quantum dots."

To achieve this effect the team employed a novel type of semiconductor to manufacture quantum dots set out like an egg carton. Tiny structures which can segregate and trap tiny quantum particles like electrons, Quantum dots play the role of the pockets in the egg carton by confining excitons, which are quasi-particles made up of an electron and a hole. Holes are made when an electron in a semiconductor is propelled to a higher energy level. The vacancy of the electron leaves a positive charge behind it. The magic happens if the hole pursues the electron to the electron's new energy state, when the two are then a single entity, know as an exciton.

In devices with little to no nonlinearity, the excitons move around unhindered and rarely meet other excitons. But if the exciton is in a quantum dot, however, it then becomes impossible to place a second identical exciton in the same egg carton pocket. To do that requires an exciton with a higher energy state, which can only be achieved with a higher energy photon. This is called a quantum blockade and is responsible for nonlinearity.

Realizing quantum dots aren't practical and on a "usable scale," as they're only a few atoms in diameter, Deng and her team designed an array of quantum dots that assisted to the nonlinearity all at once using two flakes of semiconductor. One of the flakes was tungsten disulphide while the second was molybdenum diselenide. Placed at an angle of approximately 56.5 degrees between their atomic lattices, the two intertwined electronic structures formed a bigger electronic lattice with pockets measuring about 10 atoms across.

To manipulate the array of quantum dots inside the 2D semiconductor with light, the researchers created a resonator by making one mirror at the bottom and then placing the semiconductor on top of it. Finally, the team deposited a second mirror on top of the semiconductor.

On this process, Long Zhang, a postdoctoral research fellow in the Deng Research Lab and first author on the paper, said: "You need to control the thickness very tightly so that the semiconductor is at the maximum of the optical field."

While the quantum egg carton was embedded in the mirrored cavity which allowed red laser light to resonate, the researchers noticed the emergence of another quantum state, called a polariton. These quantum particles are a hybrid of the excitons and the light in the mirrored cavity, proving all the quantum dots interact jointly with light.

"Engineers can use that nonlinearity to discern energy deposited into the system, potentially down to that of a single photon, which makes the system promising as an ultra-low energy switch," said Deng.

Deng's "switches" are among the devices required to building ultralow-power computing, which can be formed into more complex gates.

"Professor Deng's research describes how polariton nonlinearities can be tailored to consume less energy," said Michael Gerhold, program manager at the Army Research Office, an element of the U.S. Army Combat Capabilities Development Command's Army Research Laboratory. "Control of polaritons is aimed at future integrated photonics used for ultra-low energy computing and information processing that

could be used for neuromorphic processing for vision systems, natural language processing or autonomous robots."

Beyond Silicon

All this could have positive repercussions for the most crucial aspect for quantum information processing, qubits, and how every individual quantum dot in the array could be used as a qubit. Another method thrown out there would be to execute a polariton blockade, where the array of excitons, "resonating in time with the light wave", would become the qubit. These two approaches hold promise for 2D semiconductors in building more cost-effective, room-temperature quantum devices as opposed to the highly expensive cryogenic models based on liquid nitrogen or liquid helium.

The final word on this was Steve Forrest's, the Peter A. Franken Distinguished University Professor of Electrical Engineering at UM and another co-author of the paper: "We are coming to the end of Moore's Law. Two-dimensional materials have many exciting electronic and optical properties that may, in fact, lead us to that land beyond silicon."

The University of Michigan, Deng, and the other co-authors are well in the loop as to the best approaches to achieving that "lead us to that land beyond silicon" and a practical quantum computer. We have a long way to go, but research like this is one foot in the right direction.

29 US Cyber Responses to SolarWinds, Exchange Hacks

by brad d. williams

https://breakingdefense.com/2021/03/retaliation-options-us-cyber-responses-to-solarwinds-exchange-hacks/

Less than two months in office, the Biden administration is grappling with how to respond to two large-scale, widespread cyberespionage campaigns conducted by nation-states against the U.S. public and private sectors. The Cybersecurity and Infrastructure Security Agency has said that critical infrastructure operators have also been affected by the SolarWinds and Microsoft Exchange server hacking campaigns.

The administration's response to each incident will set the tone for and perhaps the trajectory of U.S. cybersecurity strategy, policy, and operations in response to adversarial national-state hacks over the next four years. The administration is said to be working on a multipronged response that will likely include a cybersecurity executive order, economic sanctions, and what National Security Advisor Jake Sullivan characterized as "tools seen and unseen."

Any cyber operations response to each incident, whatever it might entail, is fraught with difficult questions on challenging issues, such as proportionality, the risk of escalation, and "**cyber norms**," which the U.S. and many other nations advocate, but which some nations do not.

To understand the potential cyber operations "menu of options" before the administration, as well as the strategic and policy implications, Breaking Defense this week interviewed three experts with distinct insights into these matters:

- Adam Roosevelt is CEO of Arlington, Va.-based cybersecurity and intelligence firm A.R. International Consulting, a U.S. Army combat veteran, and former Department of Defense official who served in multiple roles, which included supervising military cyber activities and engaging senior military officials in support of cyber operations and exercises.

- Joe Billingsley is a Director at the National Defense University's College of Information and Cyberspace, founder of the nonprofit Military Cyber Professionals Association, and a former U.S. Army Strategist and Cyber Operations Officer. His views expressed in this article are his own and do not represent those of the U.S. government, National Defense University, or any other government agency or entity.
- Herbert Lin is Senior Research Scholar and Hank Holland Fellow at Stanford University. He co-edited, as well as co-authored essays in, the book Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.

Each section of this article explores key strategic, policy, and operations issues that will likely factor into a U.S. response, with insights into each issue provided by these experts.

What's in (and Who's Behind) A Hack?

Certainly cyberespionage campaigns are not new, but the hacks of Texas-based SolarWinds Inc. and the ongoing exploitation of four zero-day vulnerabilities in Microsoft Exchange email servers are each remarkable in their own ways.

The SolarWinds hack, which has not been formally attributed by the U.S. government but is widely thought to be the work of Russian intelligence services, is remarkable for its technical sophistication and the number of organizations impacted. Notably, U.S. Cyber Command Executive Director Dave Frederick, speaking at a virtual event this week, said there is "no evidence" Defense Department networks were compromised in the SolarWinds hack.

This week the Russian government denied any involvement in the SolarWinds hack and warned the U.S. not to respond. Reuters reporter Chris Bing tweeted on Wednesday that CISA will release further evidence attributing the hack to Russia "soon."

The Exchange hack, which Microsoft attributed to China-based HAFNIUM group as the original threat actor, is remarkable for how easy it is to exploit the four zero-day vulnerabilities, the prevalence of unpatched servers, and the reportedly high number of victims. Since Microsoft's public disclosure of the four Exchange server zero days, the FBI, CISA, and several security companies have all said multiple threat actors, in additional to HAFNIUM, are now exploiting the vulnerabilities in the wild.

Both hacking campaigns, which appear to be originally motivated by cyberespionage, were discovered during a highly uncertain presidential transition – SolarWinds in December and the Exchange exploits in early January. The SolarWinds campaign dates back to at least October 2019, when threat actors conducted a "dry run" using harmless code in SolarWinds' Orion Platform software, according to Feb. 23 Congressional testimony by FireEye CEO Kevin Mandia. FireEye first publicly disclosed the SolarWinds campaign after becoming a victim itself. While the Exchange campaign was first observed in January, it is unclear right now whether or not HAFNIUM or other threat actors had been active, yet undetected, before then.

The first question to answer in determining a response will be: Who is responsible for the hacks? Attributing hacks is notoriously difficult, especially with highly skilled threat actors such as nation-states, which is why attributions are often given along with the degree of "confidence" in the judgment. The matter is complicated by threat actors stealing and repurposing each others' tools, techniques, and procedures (TTPs), which obscures attribution even more. So, before the U.S. can respond to either incident, the government must be highly confident in its attribution.

"Russian hacker group APT 29 'Cozy Bear' is presumed to have been behind the recent SolarWinds hack," Roosevelt told Breaking Defense. "For the Biden Administration to carry out an effective cyber and intelligence operation targeting Russia, or presumably other threat actors, the administration will need to prove attribution. Presumably, APT 29 'Cozy Bear' adopts and utilizes highly competitive tradecraft in the digital domain, creating a challenge for attribution. Forensics and intelligence campaigns will provide insight on who is responsible and determine the level of force the government will use to respond to the adversary."

What Might The Potential Menu of Options Entail?

Once the U.S. government is confident in its technical attribution of the hacks, then U.S. cyber capabilities, strategy, and policy will be considered, along with the unique qualities of the nation implicated in the hack, the experts said.

From a U.S. cyber capabilities standpoint, Billingsley said, "The menu of response options is long and, to a certain extent, is only limited by creativity and the laws of physics. However, that assumes a symmetrical cyber-centric response to a cyber-centric action. All great geopolitical powers have many options at their disposal, whether cyber-centric or not."

In response to the SolarWinds campaign specifically, Roosevelt noted, "A menu of options on the table for the U.S. government will be to leverage economic sanctions as their primary weapon. The secondary menu would consider cyber options aimed at disrupting agreed-upon strategic targets in the Kremlin that serve as proving ground that the U.S. can flex its digital muscle and enforce punishment for violations."

Lin observed that the U.S. response will likely take into consideration two "constraints." Lin said, "The menu of options is broad, but they have to satisfy two constraints. First, they cannot impose a cost that might plausibly be construed as a 'use of force,' which is prohibited by the UN charter. That puts off limits a number of high-end responses, such as actions to turn off electric grids in ways that cause civilian casualties or that seriously disrupt or even damage Russian military forces. Second, they must be sufficiently painful that Russian decision-makers take note but not so painful that they provoke further escalation for which the U.S. might not be prepared."

As to the unique qualities of the nation-states formally implicated in the hacks, Billingsley said, "Many people have associated the SolarWinds hack with the Russian Federation and Exchange with the People's Republic of China. With that context in mind, we should remember that these are two vastly different global powers with a wide range of interests, trajectories, and targetable assets. In population and economy alone, one is about the tenth of the size of the other. Without direct knowledge of the current state of analysis in these cases, one can reasonably assume these are relevant topics being considered."

Lin highlighted the factors of the countries' leaders and their interests, noting, "The major difference between the SolarWinds and Exchange campaigns is that the U.S. believes the Russians are behind the first and the Chinese are behind the second. Any response has to take into account the particular character of their respective leaderships and what they value most."

Who Would Lead A U.S. Cyber Response?

If cyber operations were one of the items the administration selected from its menu of options, then the next consideration would be which entity should lead such operations and with what types of support from other entities.

Lin said, "A decision to conduct an operation of such significance should only be made at the highest levels – the White House – because of its potential for escalation. I would expect the intelligence community to be involved, including the CIA, and I suspect it would be undertaken as a covert operation rather than as a traditional military activity. I am unsure about the strategic and policy concerns being weighed in leadership, but bureaucratic and interagency concerns should also be added to that list."

Roosevelt added, "The Federal Bureau of Investigation, ODNI [Office of the Director of National Intelligence], Central Intelligence Agency, CYBERCOM, NSA, DHS, and the Department of State will work jointly together, and all have predefined roles and responsibilities. Governed by U.S. law, each agency's authorities are also outlined to ensure departments are operating within the guidelines as it pertains to investigations, countermeasures, and offensive activities. The National Policy Framework will be derived from a series of policy tools, such as the National Defense Strategy and the functional campaign plan for cyberspace operations. Given CYBERCOM's direct mission and the current focus, it is my opinion that CYBERCOM will lead the cyber operations, as its core focus is to achieve and maintain cyberspace superiority. With this in account, partner agencies will be a part of a de-facto task force."

How Do Proportionality And Cyber Norms Factor into A U.S. Cyber Operations Response?

The principles of proportionality and cyber norms are often raised in questions of retaliatory cyber operations.

As to proportionality in cyber operations, Roosevelt said, "The functional campaign plan for cyberspace operations will be leveraged in planning and executing a 'proportional offensive response.' In-house options will be discussed that focus on the capabilities of CYBERCOM, and partner agencies can jointly deploy to send a message, provided attribution can be proven. Retaliatory cyber offensive strategies must accomplish two goals: 1. send a message and 2. ensure deployed payloads are measured responses and mitigate ongoing risk to national and economic security. Considerations for measured responses will also include assessment of external factors that can lead to negative impacts on diplomatic and international security operations."

In terms of strategic and policy factors, the matter of proportionality is "a very hard question to answer," Lin observed. In regards to the SolarWinds hack specifically, Lin said, "The [New York] Times indicates that the U.S. is trying to make the argument that the Russian action was indiscriminate, whereas comparable U.S. actions are targeted. That may well be true, but if so, it rules out a U.S. response that is indiscriminate. That means any U.S. response must be targeted, and it must impose a 'proportional' cost on the target. But since there's no good analytical meaning for comparing the collective cost incurred by an indiscriminate attack to the individual cost incurred by a specifically targeted attack, in the end it will be entirely a judgment call that we will identify with the label 'proportionate' after policymakers make that judgment."

The U.S. and other countries have publicly advocated for cyber norms, including the restriction of cyberattacks against private sector entities (i.e., companies), certain public sector entities (e.g., hospitals, academic institutions, etc.), and critical infrastructure. Yet, both the SolarWinds and Microsoft Exchange server cyberespionage campaigns have affected the private sector, parts of the public sector, and critical infrastructure operators, according to the FBI, CISA, and Microsoft.

But Lin notes cyber norms may not be a factor at play here, at least based on what we know now about the SolarWinds campaign. Lin said, "To the best of anyone's knowledge to date, what has happened in SolarWinds has involved espionage – exfiltration of information from protected systems – and not attack.

That is, nothing has been damaged or destroyed or disrupted. Since the norms involve attack rather than espionage, no norms were violated at all."

What About The Risk of Escalation?

In addition to proportionality and cyber norms, a key consideration likely at play in the administration's decision-making process is the risk of escalation.

To address this, Roosevelt said, "Wargaming each scenario will include a risk assessment and map out likely outcomes of each decision. Defending forward will demand that the U.S. has a program in place to dynamically pursue leads using advanced TTPs [tools, tactics, and procedures]. The level of force is determined by assessing a series of factors that evaluate intent, capability, and outcome to deploy a measured response."

As to what a potential escalation could look like, Lin noted recent media reporting on backdoors into compromised systems that could be leveraged for more "destructive" attacks. Wednesday's FBI-CISA joint advisory also warned of this possibility.

Lin provided the following hypothetical scenario for what such an escalation could look like: "The power goes out again in Austin, Texas, during a cold-weather snap. Authorities in Texas announce that the outage is similar to the one in February, but privately through diplomatic channels to the U.S. government, the Russians claim credit for the outage and provide evidence that they have compromised the power delivery to Austin. They also provide similar evidence that they have placed similar implants in the power grids that supply five other cities in the U.S. And then they politely ask the U.S. to please refrain from sending its messages any further."

Can The U.S. Deter Future Cyberespionage And Cyberattacks?

The impossibility of "cyber deterrence" has been discussed at length in previous years, and the impossibility was accounted for and incorporated into the 2018 Command Vision for U.S. Cyber Command as the doctrine of "persistent engagement," which is related to CYBERCOM's "defend forward" concept.

Last week, CYBERCOM and NSA chief Gen. Paul Nakasone talked about "defend forward," which acknowledges the limitations of cyber deterrence and involves, he said, "executing operations outside U.S. military networks." Nakasone said "persistent engagement" is "focused on an aggressor's confidence and capabilities by countering and contesting campaigns short of armed conflict."

In light of the seeming futility of "cyber deterrence," Lin pointed to the CYBERCOM vision, which states that "Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks."

Lin said, "This is the only thing that [CYBERCOM] has said that may actually make a difference to Russian and/or Chinese activity. But, of course, that means constantly conducting offensive activity in their networks – which means they aren't responding to specific Russian or Chinese actions."

Roosevelt added that "[T]he U.S. Congress can enact laws that expand powers of CYBERCOM and intelligence agencies, allowing for streamlined decisions to disrupt adversaries following a major cyberattack."

What Else Can Be Done?

Billingsley said that Americans are "increasingly impatient" with these types of cyber campaigns carried out by nation-states against U.S. civilian targets. He added, "While there may be actions in the short-term that send messages which force adversaries to reconsider their risk appetite for a time, without wiser investments, the U.S. and its people are poised to continue being the subjects of increasingly costly cyber-related victimization at the hands of foreign entities for the foreseeable future."

Billingsley advocated long-term investment in education from K-12 through college, noting the complexities involved in understanding the current environment in cyberspace. "Despite what many may say, there is no quick fix, and we simply do not have enough Americans who understand cyberspace sufficiently," he said.

However, Billingsley does see some bright spots. "Fortunately, the U.S. is heading in a more strategically sustainable direction with efforts like the U.S. Cyberspace Solarium Commission, but a greater sense of urgency is needed across the nation to hasten the progress. Instead of waiting for taxpayer-funded programs to incentivize limited pockets of excellence, more American parents should independently prioritize STEM studies and degrees with their kids. Without such grassroots action, don't be surprised if things continue to get worse."

11 Mar 2021

30 Quantum computing: Quantum annealing versus gate-based quantum computers

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/quantum-computing-quantum-annealing-versus-gate-based-quantum-computers/

Quantum technologies have long been pitched as a way to fundamentally change the way drugs are discovered; to start putting the theory to the test, researchers from pharmaceutical company GlaxoSmithKline (GSK) have been toying with top-notch quantum devices, comparing the methods put forward by IBM and D-Wave to get a better picture of what to expect from those leading the quantum race.

The conclusion? The method used by D-Wave, called quantum annealing, can already compete against classical computers and start addressing realistic problems; on the other hand, gate-based quantum computers, such as the one that IBM is building, remain short of enough qubits to run problems that are relevant to the real world.

All is not lost for gate-based methods – quite the contrary, in fact. GSK's researchers foresee that the expected increase in qubit count in computers like these will allow quantum devices to show a significant performance advantage over classical hardware, for pharmaceutically-relevant life science problems, but also many other types of application.

The results of the scientists experiments are still in pre-print, and are yet to be certified by peer review; in addition, the trials only focus on a specific problem – the use of quantum computing to assist drug discovery. Nevertheless, the research offers a valuable overview of the capabilities of quantum devices as they stand, and of the limitations of different approaches to quantum computing.

The problem addressed by the scientists is well-established in classical computing. Called codon optimization, it consists of finding sequences of genetic code, called codons, that will ultimately lead

to the expression of a particular gene. Up to six codons can be required to represent an amino acid, which in turn form the proteins that determine the gene.

In classical computing, codon optimization is addressed with genetic algorithms (GAs) that sample and iterate many different combinations of codons before settling on the most "optimal" solution. Due to the limited capabilities of the hardware, however, GAs cannot sample a large number of solutions in little time, which is why drug discovery is a lengthy process.

"Thorough sampling of the solutions space is therefore often intractable with biologically relevant use-cases," wrote GSK's researchers.

Quantum computing, however, and the ability of qubits to carry out various calculations in parallel, shows a lot of promise for this type of optimization problem, and would allow for a larger solutions space to be explored much faster.

This is why the researchers set out to investigate the potential impact of quantum computing for codon optimization. Using a quantum algorithm, called the Binary Quadratic Model (BQM) that can run on different quantum platforms, the team decided to test two markedly different models: D-Wave's quantum annealing method, and IBM's gate-based quantum computer.

D-Wave's technology, found the researchers, holds a lot of potential. The Canadian company's 5,000-qubit Advantage system was used to run the BQM; the system was capable of mapping 30 amino acids, and when compared to the classical algorithms, it was found to achieve similar results. "(The computer) is found to be competitive in identifying optimal solutions, and future generations (...) may be able to outperform classical GAs," concluded the scientists.

Current generations of quantum hardware are not mature enough to surpass classical computing for problems such as codon optimization. In other words, D-Wave's processor did not run the calculation better than a classical algorithm; but it proved that a quantum device could perform competitively, even on a life-size problem. As the technology increases in scale, the researchers expect it to eventually outperform classical techniques.

In separate experiments, a similar conclusion was reached by researchers at materials design company OTI Lumionics, which is banking on quantum technologies to develop electronics with new properties. Using an optimization algorithm that is similar to the one run by GSK's scientists, OTI Lumionics designed a new electronic material that will let phone and laptop manufacturers build transparent, bezel-free OLED displays.

Just like GSK's team, OTI Lumionics' researchers looked at the performance of different quantum approaches when running the algorithm. They eventually settled on D-Wave, finding that, contrary to other cloud-based quantum services, the company's processor could already compete against classical methods, and reach a degree of industrial relevance.

D-Wave's quantum annealing processor, however, is only reflective of one particular branch of quantum computing: based on a system that is capable of optimizing itself to reach the lowest energy state, quantum annealing is only suited to specific optimization problems. On the other hand, it is much easier to operate and control than gate-model computers like IBM's. For this reason, D-Wave's quantum computer already boasts thousands of qubits, while IBM has only hit 65 qubits.

To compare the two methods, GSK's scientists ran the optimization algorithm on IBM's 24-qubit Qasm simulator. This limited the outcome to four amino acids; in addition, the performance of the device was variable, with many examples of the quantum algorithm returning invalid results.

According to the paper, modelling biologically-relevant sequences would require thousands of qubits with high connectivity. “Implementing a version of this program for IBM Q devices, while successful, shows that modelling practical systems requires too many qubits to be run on even the most advanced gate-based devices available (e.g. IBM’s 65-qubit Hummingbird device),” wrote the researchers.

But although they are currently less mature than quantum annealers, gate-based quantum computers are expected to significantly increase their qubit count, while also reducing error rates. IBM’s roadmap for scaling quantum technology, for example, anticipates that a 1,000-qubit system will be available by 2023.

”While current generations of devices lack the hardware requirements, in terms of both qubit count and connectivity, to solve realistic problems, future generation devices may be highly efficient,” said the researchers.

When this moment comes, the gate-based devices may be able to solve large-scale optimization problems – but also in running different types of calculations, from financial modelling to weather forecasting through traffic optimization. The range of applications that gate-based quantum computers will find, in fact, is likely to exceed that of quantum annealers. D-Wave and IBM told ZDNet they didn’t want to comment on the research.

So, while D-Wave’s quantum processor is already making strides in solving real-world problems now, a new comparison will only be fair once devices like IBM’s catch up on hardware scaling; the strengths and weaknesses of different methods will be clearer then. Until then, you can expect plenty more compare-and-contrasting from curious scientists trying to get a peek of the future.

10 Mar 2021

31 The EU wants to build its first quantum computer. That plan might not be ambitious enough

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/the-eu-wants-to-build-its-first-quantum-computer-that-plan-might-not-be-ambitious-enough/

The European Union is determined to remain a competitive player in the quantum revolution that’s expected in the next decade, and has unveiled plans to step up the development of quantum technologies within the bloc before 2030.

EU Commission vice president Margrethe Vestager and commissioner Thierry Breton have presented a new roadmap for the next 10 years, the ‘2030 digital compass’, which sets out targets for digital transformation across many different fields, in an effort to reassert the bloc’s relevance in a range of technologies.

New objectives were set for quantum technologies, with the Commission targeting a first computer with quantum acceleration by 2025, paving the way for Europe to be “at the cutting edge” of quantum capabilities by 2030.

The ultimate goal, according to the roadmap, is for the EU to be able to develop quantum computers which are highly efficient, fully programmable and accessible from anywhere in Europe, to solve in hours what can currently be solved in hundreds of days, if not years.

Sophisticated quantum computing capabilities will be used to enable faster development of new

drugs and cancer treatments, the Commission said; quantum computers will also solve highly complex optimisation problems for businesses, while helping with the design of energy-saving materials, or finding the cheapest combination of renewable sources to supply an energy grid.

Although the target is to develop the EU's first quantum computer in the next five years, the complexity of the device has not been specified. Most analysts expect that a large-scale quantum computer capable of resolving real-world problems faster than a classical device is still at least a decade away. It's likely, therefore, that the Commission is aiming for a somewhat less sophisticated device.

"It seems more likely that the quantum computer may be a noisy intermediate-scale type of quantum computer. In other words, not an all-singing-all-dancing fully fault-tolerant quantum computer, but a smaller, noisier quantum computer optimised to perform a specific computing task," Andrew Fearnside, senior associate specialising in quantum technologies at intellectual property firm Mewburn Ellis, tells ZDNet.

"That seems far more achievable to me, and also more deliverable and, therefore, more likely to show quantum-sceptical technology investors and industry that quantum computing can truly improve their business."

Alongside targets that are specific to quantum computing, the Commission also announced the goal to develop an ultra-secure quantum communication infrastructure that will span the whole of the EU. Quantum networks will significantly increase the security of communications and the storage of sensitive data assets, while also keeping critical communication infrastructure safe.

A long-standing interest

The EU's interest in quantum technologies is not new: the Commission launched a 10-year quantum flagship in 2018, which, with a €1 billion ($1.20 billion) budget, was described as one of the bloc's most ambitious research initiatives.

Since then, individual member states have started their own quantum programs: Germany, in particular, has launched a €2 billion ($2.4 billion) funding program for the promotion of quantum technologies, far surpassing many other nations; but France, the Netherlands, and Switzerland are all increasingly trying to establish themselves as hubs for quantum startups and research.

This has established Europe as a strong leader, with a high concentration of quantum-relevant talent and innovative quantum startups. However, the bloc's best efforts, in the context of a fast-moving quantum race, have not always been enough.

"When it comes to operationalising quantum technology knowledge, Europe is falling behind the US and China to create IP, secure VC funding, and establish a mature startup and industry ecosystem," Ivan Ostojic, partner at research firm McKinsey, tells ZDNet. "Europe needs to find innovative ways to accelerate the development and scaling of breakthrough applications of quantum technologies to fully capture the economic potential."

Since the US signed in the National Quantum Initiative Act in 2018, which came with a $1.2 billion budget, researchers and businesses across the Atlantic have flourished; the country is widely considered the biggest competitor in quantum, and has already established a mature ecosystem for the technology.

China, for its part, has a long-established interest in quantum technologies. Earlier this week, in fact, the Chinese government revealed its economic roadmap for the next five years, which features aggressive objectives for quantum, including the development of a long-distance and high-speed quantum

communications system, and building up computers that can support several hundred qubits.

Although the EU Commission's new roadmap reflects a desire to establish the bloc as a leading global power in quantum technologies, Ostojic argues that without a well-defined strategy, it will be difficult for Europe to compete against other nations.

"The question is if the strategy is limited to the creation of quantum computing assets, or if it includes a full ecosystem," he says. "There are critical areas to be considered across the entire value chain, from cooling technologies through quantum analytics and software to industry applications. Such a strategy should also include an answer on how to boost competitiveness from education through IP creation, company creation, funding, and industry partnerships."

Alongside the objectives it sets for quantum technologies, the Commission's roadmap lays out some aggressive milestones for the bloc in the next decade – always with a vision to establish the EU as a leading player on the international scene.

According to the document, the coronvirus crisis has highlighted Europe's "vulnerabilities" in the digital space, and the bloc's increased reliance on non-EU based technologies. The Commission aims, for example, to double the weight of European microprocessor production in the global market to reach a 20% share by 2030, up from the European semiconductor industry's current 10% share.

Similarly, the Commission highlighted that much of the data produced in Europe is stored and processed outside of the bloc, which means the EU needs to strengthen its own cloud infrastructure and capacities. By 2030, the Commission hopes that 10,000 secure edge nodes will be deployed to allow data processing at the edge of the network.

Cloud technologies have been a sticking point in the EU for many years. To resist the dominance of US-based hyperscalers, such as Microsoft and AWS, the bloc has been working on a European cloud provider dubbed GAIA-X, which launched last year, but is showing little promise of success.

The Commission's new roadmap suggests that the EU is still actively willing to claim the bloc's digital sovereignty in the face of increasing international competition. Commissioner Thierry Breton said: "In the post-pandemic world, this is how we will shape together a resilient and digitally sovereign Europe. This is Europe's Digital Decade."

The next few months will see the targets laid out in the roadmap debated and discussed, before an official 'digital compass' is adopted at the end of 2021. Then, the Commission proposes carrying out an annual review of each member states' performance in meeting the targets to keep track of the bloc's progress.

32 CQC's Cybersecurity Group's Breakthrough Makes Quantum-Safe Data and Devices Commercially Available

by Matt Swayne

https://thequantumdaily.com/2021/03/10/cqcs-cybersecurity-groups-breakthrough-makes-quantum-safe-data-and-devices-commercially-available/

When quantum computers are mentioned in the same sentence as cybersecurity or data security, it usually refers to the massive threat that quantum technology poses to current methods we use to keep our data secure.

Now, a team of Cambridge Quantum Computing scientists are showing how quantum technology can make our data and communications safe and secure not just from classical cryptographic attacks, but also from quantum-based hacking attempts. It's a step forward toward developing methods to ensure both private and national security in the quantum era.

The team – which discussed their findings in a post on Medium written by Duncan Jones, head of CQC's Quantum Cybersecurity; Alec Edgington, senior software architect and Cameron Foreman, quantum cryptography researcher – used a novel approach to generate provably-perfect entropy, which is literally unhackable, which can create quantum-proof cryptographic keys, both classical and post-quantum. They ran this entropy generation on an IonQ quantum computer, with help from the company's TKET and the Amazon Braket platform.

A truly random number generator would produce an unbiased and private stream of random bits that would be impossible to predict for a would-be hacker, according to the team. However, the standard random number generation methods are not robust enough to completely eliminate potential cyber-attacks. For example, pseudo-random number generators (PRNGs) use algorithms to expand an initial "seed" value into a random-looking sequence of bits. However, because this is deterministic, a person who figures out the seed can predict the output.

Another approach – so-called true random number generators (TRNGs) and many existing quantum random number generators (QRNG) – relies on the measurement of erratic physical systems to produce random outputs.

The researchers explain: "In a TRNG, the physical system being measured is a predominantly classical process, such as thermal noise in a diode. QRNGs observe the results of quantum processes, such as the route a photon takes when it hits an angled silvered mirror."

However, according to the team, all of these approaches cannot be fully trusted to deliver truly randomness.

The CQC team takes a third approach: using quantum computers to generate unbiased private entropy. The company calls this provable QRNG method, "IronBridge."

"Unlike the other two approaches, this is invulnerable to a quantum adversary, and it produces self-tested randomness," the researchers report.

The team's solution, which rests on the intrinsic randomness of quantum-mechanical systems, treats the quantum computer as a black box and passes it circuits to execute.

"The output of the circuits is used to generate our entropy, as well as acting as a self-test to ensure the quantum computer is functioning correctly," the researchers explain. "This means we no longer have to place complete trust in the device."

IronBridge can take imperfect – biased or not fully private – randomness and amplify it with a quantum computer, resulting in perfectly unbiased and private data with unconditional security, according to the team.

"This verified randomness and privacy amplification is only possible with quantum devices, thanks to the physical phenomenon of entanglement, which allow us to exhibit quantum effects from a device without having to characterize it," they write. "By comparing the inputs and outputs we can quantify the entanglement in the device and obtain an explicit value for the error in the device."

09 Mar 2021

33 The world's most powerful supercomputer is now up and running

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/the-worlds-most-powerful-supercomputer-is-now-up-and-running/

After seven years in the works, the world's fastest supercomputer has officially been completed in Japan and is now available for researchers to start using, for projects ranging from fighting climate change to discovering new drugs.

Builds for the **Fugaku supercomputer**, hosted at Japanese scientific research institute Riken, started in 2014 in collaboration with Fujitsu, with the device pitched to become a future pillar of the country's high-performance computing infrastructure.

The delivery of Fugaku's total 432 racks was completed in May 2020; since then, trials of the system have been on-going, mainly with projects aiming to accelerate research to combat the COVID-19 pandemic. The computer is now fully open for shared use, and Japan's **Research Organization for Information Science and Technology (RIST)** has already selected 74 research projects that will be implemented from next month.

RIST has also urged researchers to submit proposals for new projects, and invited all applications to be sent in as part of a call for Trial Access Projects.

Together with Riken, Fujitsu will continue to monitor the operation of Fugaku to ensure stable performance, while also working to enhance the user environment, and to provide better supercomputing technologies.

"The ultra-high-performance computer Fugaku is about to go into full-scale operation," said RIST president Yasuhide Tajima. "I look forward to seeing this most powerful 'external brain' ever developed by humanity helping to expand our knowledge, enabling us to gain deeper insights into the foundation of matter in both time and space, giving us better structural and functional analysis of life, society, and industry, enabling more accurate predictions; and even designing the unknown future of humanity."

Fugaku is designed to carry out high-resolution, long-duration, and large-scale simulations, and boasts up to 100 times the application performance of its predecessor, the K supercomputer, which was decommissioned in 2019.

This unprecedented compute power has earned the device the top spot for two consecutive terms in the Top500 list, which classifies the 500 most powerful computer systems around the world. At 442 petaflops, Fugaku stands a long way ahead of competitors, with three times more capability than the number two system on the list, IBM's Summit, which has a performance of 148.8 petaflops.

Paired with AI and data science, these simulations are expected to provide high-level results to solve problems at a new scale. Among the many anticipated outcomes feature high-speed and high-precision drug discovery simulations, early detection of diseases, accurate predictions and simulation of natural disasters, creation of new materials for next-generation batteries or fuel cells, and even increased insights into fundamental science questions such as the creation of the universe.

Results from the trials carried out with the supercomputer are already promising. Researchers in Japan have been using Fugaku to test the efficiency of existing drugs against Covid-19, as well as to find ways to mitigate Covid-19 transmission through detailed droplet analysis.

In a separate project, Japan's Tokyo Medical and Dental University (TMDU) and Fujitsu Laboratories

revealed that the supercomputer had enabled them to achieve cancer gene analysis in less than a day, instead of months. By allowing for a better understanding of the relationship between cancer cells and cancer-related genes, the study could help establish new cancer therapies.

"This is just the beginning for Fugaku, and we are looking forward to seeing it truly demonstrate its tremendous potential," said Riken president Hiroshi Matsumoto. "Above all, Fugaku is a key national technology, and we will manage it responsibly with the goal to achieve research results that will help build a long-lived and healthy society, disaster mitigation, and better energy use, with the ultimate goal to establish the government's vision of an ultra-smart Society 5.0."

Alongside Fugaku, Japan holds another 33 supercomputers in the latest Top500 list; and although the country has firmly settled in the top space, other nations are ramping up their efforts to develop ever-more powerful devices. The US, for example, is currently building two exascale computing systems expected to launch next year. China and the EU have also both announced projects to develop exaflop-capable supercomputers in the next few years.

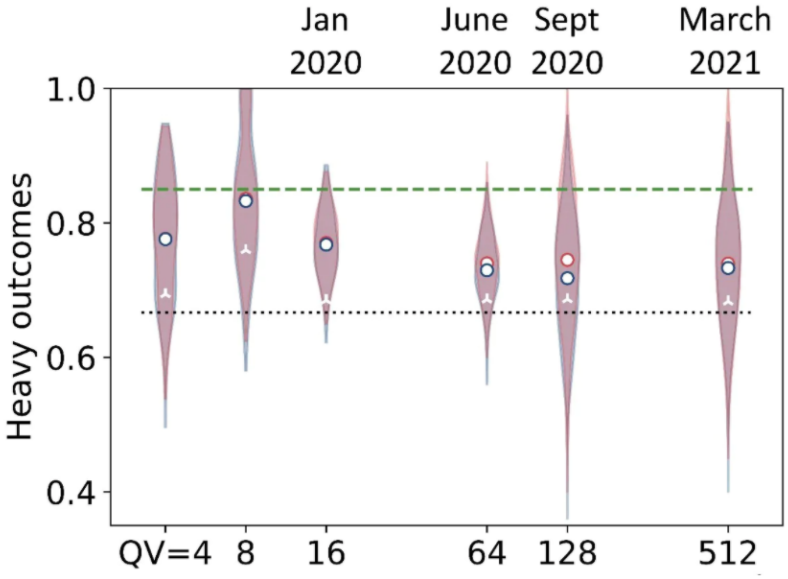
34 Honeywell Sets New Record For Quantum Computing Performance

by Matt Swayne

https://thequantumdaily.com/2021/03/09/honeywell-sets-new-record-for-quantum-computing-performance/

Honeywell Quantum Solutions reports that through performance upgrades, System Model H1 achieved a quantum volume of 512, the highest measured on a commercial quantum computer to date.

It is the third time in nine months Honeywell has set a record for quantum volume on one of its systems. Quantum volume is one way scientists measure the performance and error rates of a quantum computer. It expresses the maximum size of square quantum circuits that can be implemented successfully by the computer.



The milestone represents a four-fold increase in performance for the System Model H1, which set a record when it was released in September 2020 with a quantum volume of 128.

This high performance, combined with low error mid-circuit measurement, provides unique capabilities with which quantum algorithm developers can innovate.

According to Honeywell's research team, the average single-qubit gate fidelity for this milestone was 99.991(8)%, the average two-qubit gate fidelity was 99.76(3)% with fully-connected qubits, and measurement fidelity was 99.75(3)%. We ran 300 circuits with 20 shots each, using standard QV optimization techniques to yield an average of 76.82 two-qubit gates per circuit.

The System Model H1 successfully passed the quantum volume 512 benchmark, outputting heavy outcomes 73.32% of the time, which is above the 2/3 threshold with 99.54% confidence.

Honeywell's quantum systems are accessible directly and through ecosystem partner platforms, including Microsoft's Azure Quantum, Cambridge Quantum Computing's tket, Zapata Computing's Orquestra, and the Strangeworks QC™ platform. In addition to offering high-fidelity, fully connected qubits, our system features a unique mid-circuit measurement capability, which enables users to explore new classes of algorithms and to greatly reduce the number of qubits needed for certain algorithms.

08 Mar 2021

35 DARPA Chooses Intel, Microsoft to Quest for Cryptography's Holy Grail

by Joel Hruska

https://www.extremetech.com/computing/320616-darpa-chooses-intel-microsoft-to-quest-for-cryptographys-holy-grail

Microsoft and Intel will be working with the Defense Advanced Research Projects Agency (DARPA) to develop and implement fully homomorphic encryption (FHE) in hardware. A breakthrough in this field would have a profound impact on cybersecurity.

The encryption schemes in use today all have a common weakness: decryption. You can encrypt data any way you like, but if you want to perform useful work with it, you have to decrypt it first. Homomorphic encryption removes this problem. Not only can you compute using encrypted data, but the output of your computation also remains encrypted. A fully homomorphic encryption scheme would be capable of performing all mathematical operations on any encrypted data without the need to decrypt it.

FHE is a sort of cryptographic Holy Grail. A lot of work has been done on the topic over the past decade, but all of the current implementation methods rely on software execution rather than dedicated hardware, and they run too slowly to be of much practical use. DARPA wants to change this via its Data Protection in Virtual Environments (DPRIVE) program. The government agency has selected four research teams to pursue the question, led by Duality Technologies, Galois, SRI International, and Intel. The teams are tasked with developing a hardware accelerator for FHE that can compete with the processing speed of unencrypted algorithms. The various teams are also tasked with evaluating different word sizes rather than sticking to the 64-bit words common in modern computing.

Intel plans to tackle the problem by developing an Application Specific Integrated Circuit (ASIC) to address it. This is an interesting choice on Intel's part, given some of the work that's been done to implement FHE on Intel FPGAs. A 2019 paper by Microsoft engineers described a hypothetical FHE implementation dubbed "**HEAX**," which demonstrated substantial performance improvements over CPU-based workloads, as shown in the following tables:

FPGA Device	HE Param. Set	NTT			INTT			Dyadic MULT		
		CPU	HEAX	Speed-up	CPU	HEAX	Speed-up	CPU	HEAX	Speed-up
Arria10	Set-A	7222	89518	12.4	7568	89518	11.8	36931	1074219	29.1
Stratix10	Set-A	7222	195313	27.0	7568	195313	25.8	36931	1171875	31.7
	Set-B	3437	90144	26.2	3539	90144	25.5	18362	585938	31.9
	Set-C	1631	41853	25.7	1659	41853	25.2	9117	292969	32.1

Table 7. Performance comparison of HEAX with CPU. Number of operations per second for CKKS *low-level* operations.

FPGA Device	HE Param. Set	KeySwitch			MULT+ReLin		
		CPU	HEAX	Speed-up	CPU	HEAX	Speed-up
Arria10	Set-A	488	44759	91.7	420	44759	106.6
Stratix10	Set-A	488	97656	**200.5**	420	97656	**232.5**
	Set-B	97	22536	**232.3**	84	22536	**268.3**
	Set-C	16	2616	**163.5**	15	2616	**174.4**

Table 8. Performance comparison of HEAX with CPU. Number of operations per second for CKKS *high-level* operations.

The performance improvement from the Stratix10 FPGA implementation ranges from 25x - 232.5x faster than a conventional x86 CPU. These are significant improvements, and one can imagine that a higher-end FPGA might be able to deliver even larger gains. DARPA, however, is looking for more than a 200-300x speed improvement.

"We currently estimate we are about a million times slower to compute in the FHE world than we are in the plaintext world," said Tom Rondeau, DPRIVE's program manager. "The goal of DPRIVE is to bring FHE down to the computational speeds we see in plaintext. If we are able to achieve this goal while positioning the technology to scale, DPRIVE will have a significant impact on our ability to protect and preserve data and user privacy,"

Intel seems a bit short of FPGA's capable of delivering quite that much additional performance, so a custom ASIC design would seem to be the way to go, at least for now. Such silicon would likely be integrated on-die in a future Xeon or Core processor if the technology ever comes to the enterprise or consumer markets.

After Intel develops its implementation, Microsoft will lead the testing and commercial development by rolling the capability out across Azure. Fully homomorphic computing has significant implications for security in cloud computing environments, where there are understandable tensions between organizations that might like to use the cloud for various purposes but are leery of uploading data to third-party servers. Homomorphic encryption would resolve many of these issues.

Fully homomorphic encryption wouldn't just "fix" computer security. But it would offer an end-to-end encryption method of a type we don't currently possess. The ability to compute without first decrypting data would be a major security improvement compared with the status quo, provided we can improve the performance hit of doing so.

36 Researchers investigate 'imaginary part' in quantum resource theory

https://www.swissquantumhub.com/researchers-investigate-imaginary-part-in-quantum-resource-theory/

A research team led by the University of Science and Technology of China (USTC), has made important progress in quantum information theory.

The question of whether complex structures are necessary for quantum mechanics has long been debated by physicists. Researchers have regarded the complex number as a kind of quantum resource, and reveal

its irreplaceable role in the local discrimination of bipartite quantum states.

Using the two-photon entangled state prepared by parametric down conversion, researchers further measured and compared the success probability of locally distinguishing quantum state when only using the real measurement basis and general measurement basis. They successfully observed the increase of the success probability when using the complex measurement basis, which verified the important role of the complex in quantum mechanics.

05 Mar 2021

37 Chinese malware may have targeted Indian power systems and seaports: U.S. firm

by Insights Editor

https://www.insightsonindia.com/2021/03/05/insights-into-editorial-chinese-malware-may-have-targeted-indian-power-systems-and-seaports-u-s-firm/

Chinese state-sponsored actors may have deployed malware into Indian power grids and seaports as border tensions between India-China began escalating in May last, culminating in a deadly clash along the Line of Actual Control (LAC) in mid-June.

The alleged cyber intrusion was discovered and revealed by U.S. cyber security and intelligence firm, Recorded Future, according to the New York Times, which broke the story.

An recent grid failure in Mumbai may have been caused by the Chinese malware, as per the report.

China refuted reports that it had initiated cyber attacks against India's power grid resulting in massive power outages and also claimed that it is 'firmly opposed' to such irresponsible and ill-intentioned practices.

Recorded Future, a Massachusetts-based company that studies the use of the Internet by state actors, in its recent report details the campaign conducted by a China-linked threat activity group RedEcho targeting the Indian power sector.

About Cyber attacks

(i) Cyber-attacks are defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."

(ii) Cyber exploitation or cyber espionage, on the other hand, refers to the penetration of adversary computers and networks to obtain information for intelligence purposes; this is espionage, not a destructive activity.

(iii) Cyber-attack weapons are easy to use and they can generate outcomes that range from the simple defacing of a web site to the stealing of data and intellectual property, espionage on target systems and even disruption of critical services.

(iv) Likewise, cyber-attack as a mode of conflict raises many operational issues.

  (a) For example, how will a country know whether it is the subject of a deliberate cyber attack launched by an enemy government?

(b) How will it prove this?

(v) Proving attribution in cyberspace is a great challenge. It is extremely difficult to attribute cyber-attacks to a nation-state, since collecting irrefutable evidence has proved elusive in almost all cases of this nature in recent years.

(vi) The very nature of botnets and zombies makes it difficult to do so. This has led many analysts to conclude that the Internet is the perfect platform for plausible deniability.

(vii) Cyber attackers can support military operations. They can disrupt the target's command, control, and communications.

(viii) They can support covert actions to influence governments, events, organizations, or persons, often disguising whoever is launching those actions.

(ix) Valuable information and state secrets can be obtained through cyber espionage.

Mechanism for Cyber Attacks

Cyber-attacks can be carried out in a number of ways. Among them:

(i) Computer-network attacks

(ii) Supply-chain attacks

(iii) Social-networking-led attacks

(iv) Attacks on radio networks for GPS and wireless networks

(v) Radio frequencies with sufficiently high power to disrupt all unprotected electronics in a given geographical area

Types of cyber threats against nations

(i) Cyberattacks can be launched against the critical infrastructure of nations that includes telecommunications, energy, financial networks, transportation systems, and water distribution, among others.

(ii) In many countries, such infrastructure is owned and operated by the private sector. Much of it depends on SCADA systems, which are computer-controlled in a networked environment.

(iii) Taking advantage of vulnerabilities in these systems, attackers can disable them and disrupt essential services.

(iv) An attack on the air traffic control system could not just wreak havoc with flight schedules but also, in the worst case, cause crashes.

(v) The effects are the same as if the infrastructure were bombed or attacked by some other physical measure, without the enemy coming in by air, sea, or land. Likewise, financial networks can be targeted to disrupt a nation's economy.

(vi) Banks, stock exchanges, trading, online payment systems, and other transactions of all kinds can be brought to a grinding halt as if these were physically bombed. This is cyber war or information warfare.

(vii) The effects are similar to what would be achieved by Weapons of Mass Destruction (WMD).

Therefore, Necessity of Cyber-Security

(i) Photos, videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.

(ii) Companies have a lot of data and information on their systems. A cyber attack may lead to loss of competitive information (such as patents or original work), loss of employees/customers private data resulting into complete loss of public trust on the integrity of the organization.

(iii) A local, state or central government maintains huge amount of confidential data related to country (geographical, military strategic assets etc.) and citizens.

(iv) Unauthorized access to the data can lead to serious threats on a country.

As we choose to stay connected, we are moving towards proliferation and assimilation of larger data sets, interacting with one another (big data, machine learning, Artificial Intelligence, Internet of Things); this opens the entire ecosystem to larger threats from social deviants.

It is on the individuals as well as the body corporates to preserve the confidentiality, integrity of data, while ensuring that accessibility to the very data is not compromised on any front.

Conclusion

Cyber space infringement is a battle that we fight on everyday basis. India needs stringent laws and policy in place to combat these issues.

The extant legal framework does not sufficiently address the concerns of the sector, and there is an imminent requirement to have a comprehensive legislation in place to address the concerns.

The proactive vigilance observed by the body corporates and private individuals, is also being supported by the insurance industry, where cyber-security insurances have garnered immense popularity, and are augmenting the lack of an effective legal regime.

As we welcome the impending legislation, companies in the healthcare and the banking & financial services sector are ensuring that they rely on their own technical and organizational security measures to ensure that the data available with them is not corrupted or is subject to any unwarranted and unauthorized access.

It is oft said that the future is a click away, it is important that the click does not lead to any pernicious portal.

04 Mar 2021

38 Over 2,700 cyber attacks launched against China, Chinese security company 360 found

by Global Times

https://www.globaltimes.cn/page/202103/1217364.shtml

Chinese internet security company 360 has detected at least 40 high-level overseas hacker organizations and more than 2,700 advanced cyber attacks against China in the past few years, said the company's founder.

Zhou Hongyi, a member of the National Committee of the Chinese People's Political Consultative Conference (CPPCC) and founder and chairman of internet security company 360, made the remarks on Thursday.

His comments came after Microsoft blamed a Chinese hacking group for attacking its mail server software and a Reuters's report citing Goldman Sachs-backed cyber intelligence firm Cyfirma claiming that a "Chinese state-backed" hacking group had attacked two Indian vaccine producers in recent weeks.

Industry observers said the aforementioned allegations are pure slander as it is a highly complicated and sensitive process to figure out the origins of cyberattacks, instead data and facts have demonstrated that China is the real victim of cyberattacks.

Some Chinese cybersecurity insiders reached by the Global Times said they are not surprised by this round of accusations made by Western media using the same old trick of tarnishing China with cybersecurity issues.

Previously the 360 security company had discovered a series of attacks against China's aerospace, scientific research institutions, petroleum industry and large-scale internet companies by a hacking organization affiliated with the CIA for over a decade.

Some countries such as the US have been claiming they are the victim of cyberattacks but evidence shows it has always been a habitual perpetrator, said Qin An, head of the Beijing-based Institute of China Cyberspace Strategy.

Facts have shown that the US has been a frequent source of hacking. In June 2019, the US called off a military strike against Iran but conducted cyberattacks instead, targeting multiple Iranian computer systems, the New York Times reported in June.

Wang Wenbin, spokesperson of Chinese Foreign Ministry, said on Wednesday that China firmly opposes and combats cyberattacks and cyber theft in all forms. This position is consistent and clear.

China has reiterated on multiple occasions that given the virtual nature of cyberspace and the fact that there are all kinds of online actors who are difficult to trace, tracing the source of cyberattacks is a complex technical issue, Wang said, stressing that pinning the label of cyberattacks to a certain government is not appropriate.

He said relevant media and companies should adopt a professional and responsible attitude and underscore the importance of having sufficient evidence when identifying cyber-related incidents, rather than make groundless accusations.

39 Prime-factor mathematical foundations of RSA cryptography 'broken', claims cryptographer

by John Leyden

https://portswigger.net/daily-swig/prime-factor-mathematical-foundations-of-rsa-cryptography-broken-claims-cryptographer

Claims by a respected German mathematician that the widely used RSA algorithm has been cracked by an advance in cryptoanalysis have received a respectful but cautious response.

Trapdoor one-way functions that form the basis of most cryptographic algorithms rely for their security on the difficulty of solving some problems even with access to a powerful computer. The security of RSA, for example, relies on the difficulty of factoring the product of two large prime numbers.

Other types of cryptography use the mathematics of elliptic curves to create a one-way function that is impractical to unravel except through a brute force attack that involves trying every possible key.

'Shortest vector'

A paper from mathematician and cryptographer Claus Schnorr claims that prime factorization can be reduced to a much less intractable 'shortest vector' problem.

The abstract to the paper, entitled 'Fast Factoring Integers by SVP Algorithms', claims that this process "destroys the RSA cryptosystem".

If verified, the technique would work even if longer key values were deployed. Increasing the key length is the standard response to making sure algorithms stay ahead of advances in computing technology.

If true, a great number of secure systems that rely on RSA would become insecure or at least vulnerable to a previously well defended vector of attack.

The finding is yet to comprehensively demonstrated much less proved, and cautious interest rather than alarm was the general reaction from cryptoanalysis-savvy social media users.

Cryptographer Matthew Green commented on Twitter: "I think the general consensus (paraphrasing a few things people have said) is that this is an exciting approach that unfortunately has no practical evidence of efficacy, and the association of a particular researcher's name with it should not be viewed as changing any of that."

Professor Alan Woodward, a computer scientist at the University of Surrey, told The Daily Swig that the paper deserves "careful consideration".

"I don't believe the paper proves the claims made about RSA but that doesn't mean the idea is fundamentally wrong," he added.

03 Mar 2021

40 NIST/Xanadu Researchers Report Photonic Quantum Computing Advance

by John Russell

https://www.hpcwire.com/2021/03/03/nist-xanadu-researchers-report-photonic-quantum-computing-advance/

Researchers from the National Institute of Standards and Technology (NIST) and Xanadu, a young Canada-based quantum computing company, have reported developing a full-stack, photonic quantum computer able to carry out three important quantum algorithms, including one useful in quantum chemistry and another for graph similarity. Their work is published in Nature today.

Photonic-based quantum computing has received somewhat less attention than superconducting and trapped ion-based systems. Photonic quantum computing advocates say it has advantages over other approaches, not least is the room temperature operation of photonic chips and reduced susceptibility to some of the noise vulnerabilities associated with other qubit technologies. That said the photon detectors require cryogenic temperatures although overall the apparatus is still less complicated and cumbersome than what's required for other qubit technologies.

Xanadu has a good short video describing the tech. Briefly, there are three components to the system:

(i) squeezer

(ii) interferometer, and

(iii) photon detector.

Using laser input, the squeezers (resonators) generate a special quantum state, a squeezed state, essentially forming the qubits (of superposed photons). The qubits are carried via a wave guide through a network or beam splitters and phase shifters which comprise the interferometer. Think of the interferometer as the controllable set of gates applied to the qubits. The outputs are entangled photons whose state and number is counted and interpreted.

The researchers write in their paper:

> "Present day photonic quantum computers have been limited either to non-deterministic operation, low photon numbers and rates, or fixed random gate sequences. Here we introduce a full-stack hardware-software system for executing many-photon quantum circuits using integrated nanophotonics: a programmable chip, operating at room temperature and interfaced with a fully automated control system. It enables remote users to execute quantum algorithms requiring up to eight modes of strongly squeezed vacuum initialized as two- mode squeezed states in single temporal modes, a fully general and programmable four-mode interferometer, and genuine photon number-resolving readout on all outputs.
>
> "Multi-photon detection events with photon numbers and rates exceeding any previous quantum optical demonstration are made possible by strong squeezing and high sampling rates. We verify the non-classicality of the device output, and use the platform to carry out proof-of-principle demonstrations of three quantum algorithms: Gaussian boson sampling, molecular vibronic spectra, and graph similarity."

The researchers note that until now, no photonic machine has been demonstrated that is simultaneously dynamically programmable, readily scalable to hundreds of modes and photons, and able to access a class of quantum circuits that could not, when the system size is scaled, be efficiently simulated by classical hardware. They write, "We report results from a new device based on a programmable nanophotonic chip

which includes all of these capabilities in a single scalable and unified machine ... While our device, at its current scale, can be readily simulated by a classical computer, the architecture and platform developed can potentially enable future generations of such machines to exit this regime and perform tasks that are not practically simulable by classical systems."

The researchers ran tests around three classes of problems – **Gaussian boson sampling**, **vibronic spectra**, and **graph similarity** – and the results are best read directly in the paper. All three approaches show promise for being able, when run on quantum computers, to solve problems beyond the capacity of classical computers. The researchers were encouraged on all fronts but acknowledge the scale of their work now is not beyond classical computers.

The recent work is significant although as pointed out by Ulrik Andersen in a Nature news article in the same issue containing the paper, "Without doubt, the authors' demonstration of quantum sampling on a programmable photonic chip using highly squeezed states is remarkable and represents a milestone in this field. However, the number of commercial applications that can be implemented using the current architecture is limited. Completely different platforms are required to run heftier algorithms, such as Shor's algorithm for factoring large numbers into prime numbers, in an error-free manner. Fortunately, such platforms (also based on squeezed states) have been proposed, and their implementation constitutes the next step towards constructing a full-blown optical quantum computer."

Scaling up is an important consideration noted by the researchers: "An important factor in assessing the viability of the platform presented is the scalability of this approach. What improvements to the platform and design are required in order to scale the system size to a level where quantum advantage could potentially be achieved? To answer this, we fix a target of 100 modes, which in our architecture would require: 50 squeezers operating with squeezing factors of $r \approx 1$, a universal 50-spatial-mode interferometer, and 100 PNR detector channels. We also stipulate, as a rough estimate, that such a machine should incur no more than 3 dB of loss in the interferometer; this criterion is especially demanding, since the interferometer loss scales with the number of modes. Events with hundreds of photons would be detectable with such a machine."

The researchers suggest a number of manufacturing improvements which would move them closer to the goal. It will be interesting to monitor Photonics-based quantum computing's progress as several companies and working in the area.

Excerpt from the paper describing the apparatus details:

- A custom modulated pump laser source producing a regular pulse train (100 kHz repetition rate) of 1.5ns duration rectangular pulses.
- An electrically and optically packaged chip that synthesizes a programmable eight-mode Gaussian state with temporal mode characteristics appropriate for photon number resolving readout.
- A locking system which serves to align and stabilize the resonance wavelengths of the on-chip squeezer resonators.
- An array of digital-to-analog converters (DACs) for programming phase shifter voltages on the chip.
- An array of low-loss (off-chip) wavelength filters to sup- press unwanted light, passing only wavelengths close to the signal and idler for detection.

- A detection system, which consists of an array of eight transition-edge sensor (TES) detectors for photon number-resolving readout, and the auxiliary equipment required to operate and acquire data from them.

41 Israel Allocates $60Million to Build First Quantum Computer

by Yaacov Benmeleh

https://www.bloomberg.com/news/articles/2021-03-03/israel-allocates-60-million-to-build-first-quantum-computer

Israel is seeking to build its first quantum computer, joining a global race for one of the world's most important emerging technologies.

The Ministry of Defense and Innovation Authority are taking bids from multinational companies, Israeli businesses and universities for a 198 million-shekel ($60 million) project to build a computer with 30 to 40 qubits, according to Aviv Zeevi, vice president at the Authority's Technological Infrastructure Division. He expects the winner of the tender to begin work before the end of the year.

"We want to be in the game," Zeevi said. "We need to be at least at a reasonable level to be able to develop" varying kinds of hardware and software associated with quantum computers.

Rather than storing information in binary 0s or 1s, like classical computers, a quantum computer's qubits can be both 0 and 1 simultaneously, which translates into an exponential edge in computing power. In 2019, Google said that its quantum computer solved a problem in minutes that would take the fastest supercomputer about 10,000 years.

The new project is part of Israel's 1.25 billion shekel national initiative to build up quantum proficiency. While scientists say practical, widespread applications for quantum computers are still years away, countries like China, the U.S. and Germany are devoting large sums to figure out how to master this technology.

Israel is a tech powerhouse that's home to several dozen so-called unicorns, or privately owned tech firms worth over $1 billion. But there are only a handful of quantum computing startups, such as the software firm Classiq Technologies and Quantum Machines, which develops hardware and software for quantum computers.

The government initiative "is a massive first step," said Itamar Sivan, chief executive officer of Quantum Machines. "Our hope is that with continued investments we can grow the burgeoning quantum ecosystem here."

42 Interconnected sectors raise need for robust cyber defence strategy

by Pranav Mukul

https://indianexpress.com/article/business/economy/security-watch-interconnected-sectors-raise-need-for-robust-cyber-defence-strategy-7211796/

Even as contradictory claims emerge from the Centre and the Maharashtra government over the involvement of Chinese actors in the Mumbai power outage of October last year, the allegations have put focus on the need for India to be better prepared to protect its critical infrastructure against globally rising cyber-attack attempts on key infrastructure. Cybersecurity experts pointed out that this is particularly significant given

the increasing interconnectedness of sectors and proliferation of entry points into the internet, which could further grow with the adaption of 5G.

A National Cyber Security Strategy is being formulated by the Office of National Cyber Security Coordinator at the National Security Council Secretariat. A strategy document prepared by an inter-ministerial task force involving representatives from different central government ministries and departments has now been forwarded to an Empowered Technology Group for consultation. Once the process is through, the document will be placed before the Cabinet Committee on Security for deliberations and approval.

Hackers targeting critical infrastructure is not a new trend but experts believe that propensity for damage is more than ever, especially with countries investing in cyber offensive capabilities. In 2015, in what was the first known successful cyber attack on a power grid, hackers compromised systems of three energy distribution companies in Ukraine thereby disrupting electricity supply.

"Critical infrastructure is getting digitised in a very fast way – this includes financial services, banks, power, manufacturing, nuclear power plants, etc. Because of these a lot of security issues arise. We just saw the SolarWinds hack, which impacted national critical infrastructure in the US. Most countries are not prepared for combating the sophistication of attacks that are happening," Saket Modi, co-founder & CEO of cybersecurity firm Safe Security told The Indian Express.

"A lot of countries have started taking advantage of this. They're spending unprecedented amount of money and are building armies. Israel is a good example, they say that there is a fourth unit in the defence system, which is for defence and offence. Most countries though are not prepared, India not being an exception but there is a need for high level of preparedness because an attack can have a great impact on the economy, safety, etc," Modi added.

For the Mumbai incident, while the Centre has denied that the outage was a result of cyber attack by Chinese group Red Echo, the Maharashtra government – citing an analysis of Maharashtra Cyber Police's report by Maharashtra State Electricity Board's (MSEB) Supervisory Control and Data Acquisition system – said "there is some evidence to point at probable cyber sabotage on MSEB servers".

In addition to the Mumbai incident, Chinese actors are also said to be involved in the attack on IT systems of vaccine makers Serum Institute of India and Bharat Biotech.

There were 6.97 lakh cyber security incidents reported in the first eight months of 2020, nearly equivalent to the previous four years combined, according to information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), suggesting a surge in cyber incidents. The surge in number is perceptive since 2018 – 2.08 lakh reported incidents – and 3.94 incidents reported in 2019. In 2017, the number was 53,117 and 50,362 in 2016.

Consequently, there is also a need for an updated cybersecurity policy in the country, which the Ministry of Electronics & Information Technology is expected to come out with soon. The current cybersecurity framework put out by the government dates back to 2013. "It is important for the corporates or the respective government departments to find the gaps in their organisations and address those gaps with the help of next generation security solutions. It is essential that there is a layered security system, wherein security threat intelligence sharing is happening between different layers," said Sunil Sharma, managing director – sales (India & SAARC), at cybersecurity firm Sophos.

02 Mar 2021

43 A quantum internet is closer to reality, thanks to this switch

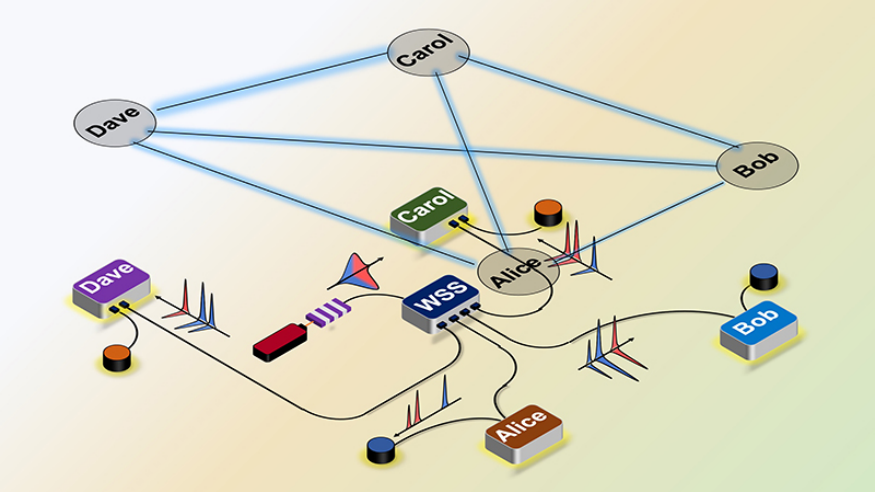
by Kayla Wiles

https://www.purdue.edu/newsroom/releases/2021/Q1/a-quantum-internet-is-closer-to-reality,-thanks-to-this-switch.html

When quantum computers become more powerful and widespread, they will need a robust quantum internet to communicate.

Purdue University engineers have addressed an issue barring the development of quantum networks that are big enough to reliably support more than a handful of users.

The method, demonstrated in a paper published in Optica, could help lay the groundwork for when a large number of quantum computers, quantum sensors and other quantum technology are ready to go online and communicate with each other.



The team deployed a programmable switch to adjust how much data goes to each user by selecting and redirecting wavelengths of light carrying the different data channels, making it possible to increase the number of users without adding to photon loss as the network gets bigger.

If photons are lost, quantum information is lost – a problem that tends to happen the farther photons have to travel through fiber optic networks.

"We show a way to do wavelength routing with just one piece of equipment – a wavelength-selective switch – to, in principle, build a network of 12 to 20 users, maybe even more," said Andrew Weiner, Purdue's Scifres Family Distinguished Professor of Electrical and Computer Engineering. "Previous approaches have required physically interchanging dozens of fixed optical filters tuned to individual wavelengths, which made the ability to adjust connections between users not practically viable and photon loss more likely."

Instead of needing to add these filters each time that a new user joins the network, engineers could just program the wavelength-selective switch to direct data-carrying wavelengths over to each new user – reducing operational and maintenance costs as well as making a quantum internet more efficient.

The wavelength-selective switch also can be programmed to adjust bandwidth according to a user's needs, which has not been possible with fixed optical filters. Some users may be using applications that require more bandwidth than others, similarly to how watching shows through a web-based streaming service uses more bandwidth than sending an email.

For a quantum internet, forming connections between users and adjusting bandwidth means distributing entanglement, the ability of photons to maintain a fixed quantum mechanical relationship with one another no matter how far apart they may be to connect users in a network. Entanglement plays a key role in quantum computing and quantum information processing.

"When people talk about a quantum internet, it's this idea of generating entanglement remotely between two different stations, such as between quantum computers," said Navin Lingaraju, a Purdue Ph.D. student in electrical and computer engineering. "Our method changes the rate at which entangled photons are shared between different users. These entangled photons might be used as a resource to entangle quantum computers or quantum sensors at the two different stations."

Purdue researchers performed the study in collaboration with Joseph Lukens, a research scientist at Oak Ridge National Laboratory. The wavelength-selective switch that the team deployed is based on similar technology used for adjusting bandwidth for today's classical communication.

The switch also is capable of using a "flex grid," like classical lightwave communications now uses, to partition bandwidth to users at a variety of wavelengths and locations rather than being restricted to a series of fixed wavelengths, each of which would have a fixed bandwidth or information carrying capacity at fixed locations.

"For the first time, we are trying to take something sort of inspired by these classical communications concepts using comparable equipment to point out the potential advantages it has for quantum networks," Weiner said.

The team is working on building larger networks using the wavelength-selective switch. The work was funded by the U.S. Department of Energy, the National Science Foundation and Oak Ridge National Laboratory.

44 Cambridge Quantum Announces Largest Ever Natural Language Processing Implementation on a Quantum Computer

by CQC

https://cambridgequantum.com/cambridge-quantum-announces-largest-ever-natural-language-processing-implementation-on-a-quantum-computer/

Cambridge Quantum Computing (CQC) announces the publication of a research paper on the online pre-print repository arxiv that provides details of the largest ever experimental implementation of Natural Language Processing (NLP) tasks on a quantum computer.

Titled "**QNLP in Practice: Running Compositional Models of Meaning on a Quantum Computer**," the paper presents the first "medium-scale" implementation of common NLP tasks. Completed on an IBM quantum computer, the experiment, which instantiated sentences as parameterised quantum circuits, embeds word meanings as quantum states which are "entangled" according to the grammatical structure of the sentence.

The paper builds on prior proof-of-concept work and, significantly, achieves convergence for the far larger datasets that are employed here. One of the objectives of the CQC team is to describe Quantum Natural Language Processing (QNLP) and their results in a way that is accessible to NLP researchers and practitioners thus paving the way for the NLP community to engage with a quantum encoding of language processing.

Bob Coecke, CQC's Chief Scientist and also the Head of CQC's QNLP project, commented, "We are working on an immensely ambitious project at CQC that is aimed at utilising quantum computers, as they scale, to move beyond expensive black-box mechanisms for NLP to a paradigm where we become more effective, more accurate and more scalable in an area of computer science that epitomises artificial intelligence. Having made considerable progress already on our 'quantum-native' brand of compositional NLP, we are now moving beyond our initial research and working on applications that can be developed in synch with timelines provided by quantum computing hardware companies such as IBM, Honeywell, Google and others."

He added, "Equally, at a time when quantum computing is becoming a topic of general interest it is imperative that those of us who are working within this sector provide results that are verifiable. Our record of publication at CQC strives at all times to meet these exacting standards – we are science led and enterprise driven."

01 Mar 2021

45 How to get started in quantum computing

by David Matthews

https://www.nature.com/articles/d41586-021-00533-x

To the untrained eye, a circuit built with IBM's online Quantum Experience tool looks like something out of an introductory computer-science course. Logic gates, the building blocks of computation, are arrayed on a digital canvas, transforming inputs into outputs.

But this is a quantum circuit, and the gates modify not the usual binary 1 or 0 bits, but qubits, the fundamental unit of quantum computing. Unlike binary bits, qubits can exist as a 'superposition' of both 1 and 0, resolving one way or the other only when measured. Quantum computing also exploits properties such as entanglement, in which changing the state of one qubit also changes the state of another, even at a distance.

Those properties empower quantum computers to solve certain classes of problem more quickly than classical computers. Chemists could, for instance, use quantum computers to speed up the identification of new catalysts through modelling.

Yet that prospect remains a distant one. Even the fastest quantum computers today have no more than 100 qubits, and are plagued by random errors. In 2019, Google demonstrated that its 54-qubit quantum computer could solve in minutes a problem that would take a classical machine 10,000 years. But this 'quantum advantage' applied only to an extremely narrow situation. Peter Selinger, a mathematician and quantum-computing specialist at Dalhousie University in Halifax, Canada, estimates that computers will need several thousand qubits before they can usefully model chemical systems.

"The stage of quantum computers now is something like classical computing in the late 1980s," says Sara Metwalli, a quantum-computing researcher at Keio University in Tokyo. "Most of the work done now is to prove that quantum, in the future, may have the ability to solve interesting problems."

Fast-moving field

Still, progress is happening fast. IBM hopes to have a 1000-qubit machine by 2023, and quantum-computing advocates enthuse that the field is ripe for development. For those who want to see what the fuss is about, a growing collection of online tutorials, programming languages and simulators are making it easier than ever to dip their toes into quantum computing.

The digital logic underlying classical computers is well known: 1 AND 0 = 0, for instance. But quantum computers are much more fluid, and researchers must come to grips with how qubit states are expressed mathematically to understand how they behave. "Quantum computing is essentially matrix vector multiplication – it's linear algebra underneath the hood," says Krysta Svore, principal manager of the quantum-computing group at Microsoft Research in Redmond, Washington.

Several online guides build up from the basics. Physicist Michael Nielsen and software engineer Andy Matuschak, both based in San Francisco, California, have produced a walk-through resource called Quantum Computing for the Very Curious. And IBM has created an interactive toolkit to accompany its Qiskit quantum language, with exercises that can be run in a Jupyter computational notebook.

Scientists also need to wrap their heads around quantum circuits, says Jeannette Garcia, senior manager for the quantum applications, algorithms and theory team at IBM Research in San Jose, California. Running from left to right and looking a bit like a musical stave, these circuits visually represent how qubits are transformed by logic gates – similar to the AND, OR and NOT gates from which electronic circuits are built – before being measured to reveal their state. IBM's Quantum Experience allows users to drag and drop logic gates to create their own circuits in a web browser, and to run them remotely on a real quantum computer.

Lingua quantum

From there, dedicated software frameworks and programming languages allow researchers to simulate, execute and explore the quantum circuits they design. Several of these languages were described in a 2020 review.

Microsoft, IBM and Google have all created tools – Q#, Qiskit and Cirq, respectively – that draw heavily on the Python programming language, and have built user-friendly development environments with ample documentation to help coders get started. Microsoft, for example, has created a full quantum development kit (QDK), containing code libraries, a debugger and a resource estimator, which checks in advance how many qubits an algorithm will require.

And it's not just the technology giants that are involved. Rigetti Computing in Berkeley, California, which has its own 31-qubit machine, has released a quantum-software development kit called Forest, which includes a Python library called pyQuil. And UK-based Cambridge Quantum Computing has launched tket, with the associated pytket library.

Another option is Silq, a language released last year by a team at the Swiss Federal Institute of Technology (ETH) in Zurich. One of its key advantages, says co-creator Benjamin Bichsel, involves 'uncomputation'. The language automatically resets the temporary values used by a quantum program, rather than forcing programmers to do this tedious work manually.

Somewhat less user-friendly is Quipper. Unlike Python, Quipper is not an 'imperative' language – one in which the program details a series of steps that change the state of the software, says Selinger, who is one of Quipper's creators. Rather, it is 'functional', more akin to a series of mathematical functions. "You never update anything, there are no variables," Selinger says.

Although not immediately useful for current small-scale devices, Quipper's functional nature could ultimately make it easier to mathematically verify that a quantum program is bug-free and actually solving the problem you want it to, Selinger says. But it also makes the language less accessible. "If you want a non-specialist, such as a chemist, to try quantum computing, then it is best to lower the threshold of entry and start with a programming language that most people are already familiar with," says Selinger. He suggests Qiskit or one of the other imperative, Python-based languages.

Actual quantum computers are largely in the hands of private technology firms, who offer access to the hardware on a variety of terms.

IBM makes a five-qubit machine freely available, but to use the company's more-powerful machines, research organizations need to be part of its Quantum Network, comprising universities, laboratories and companies. Although IBM doesn't make its pricing public, it does give out 'access awards' to scientists who have a "cool research idea and want access to a device to try it out", says Garcia. For instance, a team at the University of Chicago in Illinois, announced last November that it had used IBM's machine to explore an 'exciton condensate', a highly electrically conductive quantum system.

Microsoft offers access to other firms' quantum computers through its new Azure Quantum platform. This is at a free 'limited preview' stage, says Svore, and research institutions can apply to become early adopters.

Google doesn't sell access to its quantum machines. But Markus Hoffmann, who heads its quantum-computing partnerships and programs team, says that any scientist with a strong proposal for an experiment that could be deployed on Google's hardware should get in touch. "Based on the research impact in the field, we will find a way to make that experiment happen," says Hoffmann, who is based in Munich, Germany.

Ashley Montanaro, a quantum-computing researcher at the University of Bristol, UK, runs his quantum programs through Amazon Web Services, a cloud-computing platform that plugs into other firms' quantum devices. It costs him around US$1 to test one quantum circuit, but because researchers might want to test thousands of such circuits, "the cost can rack up", he cautions.

Start with simulations

Curious scientists can also experiment with an emulator that simulates a quantum computer on a classical machine. Microsoft's QDK, for example, has a built-in emulator that can simulate a 30-qubit device on a laptop.

"I would suggest to anyone: start on an emulator," says Thomas O'Brien, European quantum algorithms and applications lead at Google's Quantum AI research team, who is based in Munich. "[An] emulator is much more predictable. It allows you to actually see the quantum states," he says. Inspecting the state of a real quantum computer just causes it to collapse, making troubleshooting difficult, he says. And stray background heat or magnetic fields can easily knock qubits out of their existing state.

But scientists should still run their programs on a real quantum computer if they can, Montanaro advises, to get used to their noisy, error-prone behaviour. "It just tells you things that you just don't get from emulation," he says.

As research advances and quantum devices improve, such headaches will diminish. But even then, quantum computers are unlikely to replace their classical counterparts. Instead, they will sit embedded within a larger classical architecture, crunching those problems for which they provide an exponential speed-up.

Researchers still need to home in on which problems those are, but the search is on. “This is really the big question, and I think the only way to answer it is through exploration,” says Eric Johnston, co-author of Programming Quantum Computers (2019), who is based in Boston, Massachusetts. “If you’re a scientist who knows some classical computing, there is so much unexplored terrain in quantum computation that you’ll never be bored.”

46 Malware attack that crippled Mumbai’s power system came from China, claims infosec intel outfit Recorded Future

by Laura Dobberstein

https://www.theregister.com/2021/03/01/statesponsored_chinese_group_attacked_india/

Security intelligence firm Recorded Future’s Insikt Group has written a paper alleging China was behind attacks on India’s electricity grid.

In a blog post and white paper, the firm said it had seen a notable increase in targeted attacks on India from China state-sponsored groups.

The cybersecurity firm has named the offenders “**RedEcho**.”

The incident it referred to took place last year, during the India/China border standoff in May. Malware was injected into 10 Indian power sector organisations and a pair of Indian seaport operators. The attack is considered the probable source of Mumbai’s power outage in October of the same year.

“Using a combination of proactive adversary infrastructure detections, domain analysis, and Recorded Future Network Traffic Analysis, we have determined that a subset of these AXIOMATICASYMPTOTE servers share some common infrastructure tactics, techniques, and procedures (TTPs) with several previously reported Chinese state-sponsored groups, including APT41 and Tonto Team,” the Recorded Future report said. “AXIOMATICASYMPTOTE” is the name given to the malware infrastructure.

The firm said most of the malware was not activated and the associated power outage was the result of a subset of the payload. Recorded Future did not have access to India’s power system code to analyse in further detail. The cybersecurity company said it had contacted Indian authorities, which to date have largely kept quiet on the issue.

Tech-related tensions between the two nations saw India ban over 100 Chinese apps while also creating new investment funds that explicitly aim to lure major electronics manufacturers from the Middle Kingdom to India.

Recorded Future hypothesised that last year’s power outages in Mumbai, which caused mass chaos in the city’s infrastructure – ranging from trains to hospitals to financial centre operations – were a “show of force” designed to warn India of China’s capabilities.

“While diplomacy and economic factors have been effective in preventing a full-blown war, notable most recently with the bilateral disengagement at the border, cyber operations continue to provide countries with a potent asymmetric capability to conduct espionage or pre-position within networks for potentially disruptive reasons,” the report said.

47 Benchmarking quantum computers

https://www.swissquantumhub.com/benchmarking-quantum-computers/

Scientist at Atos Quantum Laboratory, France, has written an interesting paper about quantum benchmarking.

Existing protocols for benchmarking current quantum co-processors fail to meet the usual standards for assessing the performance of High-Performance-Computing platforms.

This paper introduces a new benchmark, dubbed **Atos Q-scoreTM**, that is application-centric, hardware-agnostic and scalable to quantum advantage processor sizes and beyond.

The Q-score measures the maximum number of qubits that can be used effectively to solve the MaxCut combinatorial optimization problem with the Quantum Approximate Optimization Algorithm.

They provide a robust definition of the notion of effective performance by introducing an improved approximation ratio based on the scaling of random and optimal algorithms.

They illustrate the behavior of Q-score using perfect and noisy simulations of quantum processors.

Finally, they provide an open-source implementation of Q-score that makes it easy to compute the Q-score of any quantum hardware.

48 Cybersecurity meet urges users to be better prepared to deal with threats

by staff reporter

https://www.thehindu.com/news/cities/kozhikode/cybersecurity-meet-urges-users-to-be-better-prepared-to-deal-with-threats/article33957808.ece

The two-day international cybersecurity summit organised by the Kerala Police Cyberdome drew to a close at Kozhikode on Sunday with a call to internet users to be prepared for evolving cyber-threats and to be equipped with the tools for self-defence. Targeted cyberattacks and data manipulation attempts by fraudsters were projected as huge concerns by the experts at the summit.

Delivering the keynote address, Additional Director General of Police Manoj Abraham, who is also the Nodal Officer of the Kerala Police Cyberdome, pointed out that there should be better vigil against targeted cyberattacks and the attempts to manipulate stolen data to tamper the reputation of big companies.

“Everything around us had a paradigm shift with the digital transition from the physical world. Acceleration of digital transformation has also taken place with the outbreak of COVID-19 pandemic. Cybercrimes are also increasing in pace with these rapid transitions,” said Mr. Abraham.

He said new forms of ransomware and phishing were found creating a lot of problems during the pandemic. He said people should be ready to invest more time and energy to get advanced defence tools for cybersecurity.

As many as 18 talks were held on the concluding day by experts who explained in detail the strategies to face cybersecurity threats and the loopholes to look out for. The importance of having a proper data backup plan was stressed by many of them as it would help companies minimise the impact of cyberattacks and get back on track without suffering much loss.

There was also a proposal to offer better training for employees on responsible and healthy use of digital resources at work and to prevent the possible entry of hackers. Some of the presentations pointed out that hackers were mostly found targeting individuals to get into the company network.