Crypto News

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

January 4, 2021

Contents

December 2020

31 Dec 2020

1 Tiny Quantum Computer Solves Real Logistics Optimization Problem

https://scitechdaily.com/tiny-quantum-computer-solves-real-logistics-optimization-problem/

Quantum computers have already managed to surpass ordinary computers in solving certain tasks – unfortunately, totally useless ones. The next milestone is to get them to do useful things. Researchers at Chalmers University of Technology, Sweden, have now shown that they can solve a small part of a real logistics problem with their small, but well-functioning quantum computer.

Interest in building quantum computers has gained considerable momentum in recent years, and feverish work is underway in many parts of the world. In 2019, Google's research team made a major breakthrough when their quantum computer managed to solve a task far more quickly than the world's best supercomputer. The downside is that the solved task had no practical use whatsoever – it was chosen because it was judged to be easy to solve for a quantum computer, yet very difficult for a conventional computer.

Therefore, an important task is now to find useful, relevant problems that are beyond the reach of ordinary computers, but which a relatively small quantum computer could solve.

"We want to be sure that the quantum computer we are developing can help solve relevant problems early on. Therefore, we work in close collaboration with industrial companies," says theoretical physicist Giulia Ferrini, one of the leaders of Chalmers University of Technology's quantum computer project, which began in 2018.

Together with Göran Johansson, Giulia Ferrini led the theoretical work when a team of researchers at Chalmers, including an industrial doctoral student from the aviation logistics company Jeppesen, recently showed that a quantum computer can solve an instance of a real problem in the aviation industry.

The algorithm proven on two qubits

All airlines are faced with scheduling problems. For example, assigning individual aircraft to different routes represents an optimization problem, one that grows very rapidly in size and complexity as the number of routes and aircraft increases.

Researchers hope that quantum computers will eventually be better at handling such problems than today's computers. The basic building block of the quantum computer – the qubit – is based on completely different principles than the building blocks of today's computers, allowing them to handle enormous amounts of information with relatively few qubits.

However, due to their different structure and function, quantum computers must be programmed in other ways than conventional computers. One proposed algorithm that is believed to be useful on early quantum computers is the so-called Quantum Approximate Optimization Algorithm (QAOA).

The Chalmers research team has now successfully executed said algorithm on their quantum computer – a processor with two qubits – and they showed that it can successfully solve the problem of assigning aircraft to routes. In this first demonstration, the result could be easily verified as the scale was very small – it involved only two airplanes.

Potential to handle many aircraft

With this feat, the researchers were first to show that the QAOA algorithm can solve the problem of assigning aircraft to routes in practice. They also managed to run the algorithm one level further than anyone before, an achievement that requires very good hardware and accurate control.

"We have shown that we have the ability to map relevant problems onto our quantum processor. We still have a small number of qubits, but they work well. Our plan has been to first make everything work very well on a small scale, before scaling up," says Jonas Bylander, senior researcher responsible for the experimental design, and one of the leaders of the project of building a quantum computer at Chalmers.

The theorists in the research team also simulated solving the same optimization problem for up to 278 aircraft, which would require a quantum computer with 25 qubits.

"The results remained good as we scaled up. This suggests that the QAOA algorithm has the potential to solve this type of problem at even larger scales," says Giulia Ferrini.

Surpassing today's best computers would, however, require much larger devices. The researchers at Chalmers have now begun scaling up and are currently working with five quantum bits. The plan is to reach at least 20 qubits by 2021 while maintaining the high quality.

2 Quantum Teleportation Was Just Achieved With 90% Accuracy Over a 44km Distance

by DAVID NIELD

https://www.sciencealert.com/scientists-achieve-sustained-high-fidelity-quantum-teleportation-over-44-km/amp

Scientists are edging closer to making a super-secure, super-fast quantum internet possible: they've now been able to 'teleport' high-fidelity quantum information over a total distance of 44 kilometres (27 miles).

Both data fidelity and transfer distance are crucial when it comes to building a real, working quantum internet, and making progress in either of these areas is cause for celebration for those building our next-generation communications network.

In this case the team achieved a greater than 90 percent fidelity (data accuracy) level with its quantum information, as well as sending it across extensive fibre optic networks similar to those that form the backbone of our existing internet.

"We're thrilled by these results," says physicist Panagiotis Spentzouris, from the Fermilab particle physics and accelerator laboratory based at the California Institute of Technology (Caltech).

"This is a key achievement on the way to building a technology that will redefine how we conduct global communication."

Quantum internet technology uses qubits; unmeasured particles that remain suspended in a mix of possible states like spinning dice yet to settle.

Qubits that are introduced to one another have their identities 'entangled' in ways that become obvious once they're finally measured. Imagine these entangled qubits as a pair of dice - while each can land on any number, they are both guaranteed to add to seven no matter how far apart they are. Data in one location instantly reflects data in another.

By clever arrangement of entangling three qubits, it's possible to force the state of one particle to adopt the 'dice roll' of another via their mutually entangled partner. In quantum land, this is as good as turning one particle into another, teleporting its identity across a distance in a blink.

The entanglement still needs to be established in the beginning though, and then maintained as the qubits are sent to their eventual destination through optical fibres (or satellites).

The unstable, delicate nature of quantum information makes it tricky to beam entangled photons over long distances without interference, however. Longer optical fibres simply mean more opportunity for noise to interfere with the entangled states.

In total, the lengths of fibre used to channel each cubit added to 44 kilometres, setting a new limit to how far we can send entangled qubits and still successfully use them to teleport quantum information.

It's never before been demonstrated to work over such a long distance with such accuracy, and it brings a city-sized quantum network closer to reality – even though there are still years of work ahead to make that possible.

"With this demonstration we're beginning to lay the foundation for the construction of a Chicago-area metropolitan quantum network," says Spentzouris.

Quantum entanglement and data teleportation is a complex science, and not even the experts fully understand how it might ultimately be used in a quantum network. Each proof of concept like this that we get puts us a little closer to making such a network happen though.

As well as promising huge boosts in speed and computational power, a quantum internet would be ultra-secure – any hacking attempt would be as good as destroying the lock being picked. For now at least, scientists think quantum internet networks will act as specialist extensions to the classical internet, rather than a complete replacement.

Researchers are tackling quantum internet problems from all different angles, which is why you'll see a variety of distances mentioned in studies – they're not all measuring the same technology, using the same equipment, to test the same standards.

What makes this study special is the accuracy and the distance of the quantum entanglement teleportation, as well as the 'off the shelf' equipment used – it should theoretically be relatively easy to scale up this technology using the hardware we're already got in place.

"We are very proud to have achieved this milestone on sustainable, high-performing and scalable quantum teleportation systems," says physicist Maria Spiropulu, from Caltech.

"The results will be further improved with system upgrades we are expecting to complete by the second quarter of 2021."

3 IBM Makes Encryption Paradox Practical

by Dan Garisto

https://spectrum.ieee.org/tech-talk/computing/software/ibm-makes-cryptographic-paradox-practical

How do you access the contents of a safe without ever opening its lock or otherwise getting inside? This riddle may seem confounding, but its digital equivalent is now so solvable that it's becoming a business plan.

IBM is the latest innovator to tackle the well-studied cryptographic technique called fully homomorphic encryption (FHE), which allows for the processing of encrypted files without ever needing to decrypt them first. Earlier this month, in fact, Big Blue introduced an online demo for companies to try out with their own confidential data. IBM's FHE protocol is inefficient, but it's workable enough still to give users a chance to take it for a spin.

Today's public cloud services, for all their popularity, nevertheless typically present a tacit tradeoff between security and utility. To secure data, it must stay encrypted; to process data, it must first be decrypted. Even something as simple as a search function has required data owners to relinquish security to providers whom they may not trust.

Yet with a workable and reasonably efficient FHE system, even the most heavily encrypted data can still be securely processed. A customer could, for instance, upload their encrypted genetic data to a website, have their genealogy matched and sent back to them – all without the company ever knowing anything about their DNA or family tree.

At the beginning of 2020, IBM reported the results of a test with a Brazilian bank, which showed that FHE could be used for a task as complex as machine learning. Using transaction data from Banco Bradesco, IBM trained two models – one with FHE and one with unencrypted data – to make predictions such as when customers would need loans.

Even though the data was encrypted, the FHE scheme made predictions with accuracy equal to the unencrypted model. Other companies, such as Microsoft and Google have also invested in the technology and developed open-source toolkits that allow users to try out FHE. These software libraries, however, are difficult to implement for anyone but a cryptographer, a problem IBM hopes to remedy with its new service.

"This announcement right now is really about making that first level very consumable for the people [who] are maybe not quite as crypto-savvy," said Michael Osborne, a security researcher at IBM.

One of the problems with bringing FHE to market is that it must be tailor-made for each situation. What works for Banco Bradesco can't necessarily be transferred seamlessly over to Bank of America, for example.

"It's not a generic service," said Christiane Peters, a senior cryptographic researcher at IBM "You have to package it up. And that's where we hope from the clients that they guide us a little bit."

It is not clear whether IBM's scheme for FHE is any better than that of its competitors. However, by offering a service to clients, the company may have gotten the lead on tackling some of the first practical implementations of the technology, which has been in development for years.

Since the 1970s, cryptographers had considered what it would mean to process encrypted data, but no one was sure whether such an encryption scheme could exist even in theory. In 2009, Craig Gentry, then a Stanford graduate student, proved FHE was possible in his PhD dissertation.

Over the past decade, algorithmic improvements have improved the efficiency of FHE by a factor of about a billion. The technique is still anywhere from 100 to a million times slower than traditional data processing – depending on the data and the processing task. But in some cases, Osborne says, FHE could still be attractive.

One way to understand a key principle behind FHE is to consider ways in which an adversary might break it. Suppose Alice wants to put her grocery list on the cloud, but she's concerned about her privacy. If Alive encrypts items on her list by shifting one letter forward, she can encode APPLES as BQQMFT. This is easily broken, so Alice adds noise, in the form of a random letter. APPLES instead becomes BQQZMFT. This makes it much, much harder for the attacker to guess the grocery items because they have to account for noise. Alice must strike a balance: too much noise and operations take too much time; too little noise and the list is unsecured. Gentry's 2009 breakthrough was to introduce a specific, manageable amount of noise.

While FHE may be of interest to many individual consumers interested in data privacy, its early corporate adopters are mainly limited to the finance and healthcare sectors, according to Peters.

FHE's applications may be increasing with time, though. In a data-rich, privacy-poor world, it's not hard to recognize the appeal of a novel technology that lets people have their secret cake and eat it too.

30 Dec 2020

4 Major Quantum Computing Projects and Innovations of 2020

by Shraddha Goled

https://analyticsindiamag.com/major-quantum-computing-projects-and-innovations-of-2020/

Quantum computing has opened multiple doors of possibilities for quick and accurate computation for complex problems, something which traditional methods fail at doing. The pace of experimentation in quantum computing has very naturally increased in recent years. 2020 too saw its share of such breakthroughs, which lays the groundwork for future innovations. We list some of the significant quantum computing projects and experiments of 2020.

Atos Develops Q-Score to Assess Quantum Performance

IT services company Atos devised Q-Score for measuring quantum performance. As per the company, this is the first universal quantum metric that applies to all programmable quantum processors. The company said that in comparison to qubits, the standard figure of merit for performance assessment, Q-Score provides 'explicit, reliable, objective, and comparable results when solving real-world optimisation problems'.

The Q-Score is calculated against three parameters: application-driven, ease of use, and objectiveness and reliability.

Largest-Ever Chemical Experiment For Quantum Computing

Google's AI Quantum team performed the largest chemical simulation, to date, on a quantum computer. Explaining the experiment in a paper titled, "Hartree-Fock on a superconducting qubit quantum computer," the team said it used variational quantum eigensolver (VQE) to simulate chemical mechanisms using quantum algorithms.

It was found that the calculations performed in this experiment were two times larger than the previous similar experiments and contained about ten times the number of quantum gate operations.

Algorithm to Characterise Noise in Quantum Computers

The University of Sydney developed an algorithm for characterising noise in large scale quantum computers. Noise is one of the major obstacles in building quantum computers. With this newly developed algorithm, they have tried to tame the noise by reducing interference and instability.

A new method was introduced to return an estimate of the effective noise with relative precision. The method could also detect all correlated errors, enabling the discovery of long-range two-qubit correlations in the 14 qubit device. In comparison, the previous methods would render infeasible for device size above 10 qubits.

The tool is highly scalable, and it has been tested successfully on the IBM Quantum Experience device. The team believes that with this, the efficiency of quantum computers in solving computing problems will be addressed.

Commercialised Quantum Computing

Canadian quantum computing D-Wave Systems announced the general availability of its next-generation quantum computing platform. This platform offers new hardware, software, and tools for accelerating the delivery of quantum computing applications. The platform is now available in the Leap quantum cloud service and has additions such as Advantage quantum system with 5000 qubits and 15-way qubit connectivity.

It also has an expanded solver service that can perform calculations of up to one million variables. With these capabilities, the platform is expected to assist businesses that are running real-time quantum applications for the first time.

Majorana Fermions

Physicists at MIT reported evidence of Majorana fermions on the surface of gold. Majorana fermions are particles that are theoretically their own antiparticle; it is the first time these have been observed on metal as common as gold. With this discovery, physicists believe that this could prove to be a breakthrough for stable and error-free qubits for quantum computing.

The future innovation in this direction would be based on the idea that combinations of Majorana fermions pairs can build qubit in such a way that if noise error affects one of them, the other would still remain unaffected, thereby preserving the integrity of the computations.

Intel Introduced Horse Ridge II

In December, Intel introduced Horse Ridge II. It is the second generation of its cryogenic control chip, considered a milestone towards developing scalable quantum computers. Based on its predecessor, Horse Ridge I, it supports a higher level of integration for the quantum system's control. It can read qubit states and control several gates simultaneously to entangle multiple qubits. One of its key features is the Qubit readout that provides the ability to read the current qubit state.

With this feature, Horse Ridge II allows for faster on-chip, low latency qubit state detection. Its multigate pulsing helps in controlling the potential of qubit gates. This ability allows for the scalability of quantum computers.

28 Dec 2020

5 Japanese firms explore quantum cryptography to make stock trading secure

https://japantoday.com/category/tech/japanese-firms-explore-quantum-cryptography-to-make-stock-trading-secure-1

A group of Japanese firms has launched the country's first study into quantum cryptography in a bid to enhance the security of stock trading.

The joint study, commenced the same day by Toshiba Corp, NEC Corp and Nomura Holdings Inc among others, comes amid increasing threats from cyberattacks on financial institutions.

Quantum cryptography, in theory, is considered to be impossible for third parties to crack, the group said. The companies expect to put the technology into use in stock trading within several years.

In the joint research, they will connect a cryptographic device developed by Toshiba to a trading system at Nomura Securities Co, the brokerage unit of Nomura Holdings, and test run encryption using virtual customer details and trading data.

The simulations, conducted with a help from the National Institute of Information and Communications Technology, will look into the ability to encrypt numerous orders without delay even when millions of orders are made simultaneously, they said. It will also check if there is any impact on the system when operations stretch for days.

26 Dec 2020

6 Quantum Outlook for 2021 – A Breakout Year

https://quantumcomputingreport.com/quantum-outlook-for-2021-a-breakout-year/

Despite all the inconveniences created by the Covid pandemic, a lot of progress was made in all quantum areas in 2020. We had forecasted many of them a year ago in our Quantum Computing Outlook for 2020, but there still were a few surprises. and, We did not forsee the Coronavirus at the time but we did follow up in March with a report on Coronavirus and Quantum Computing. Our hats are off to all the hard working scientists and engineers who were able to make outstanding progress while working from home.

Looking ahead to 2021, we believe that it will be a breakout year for quantum computing. The pace of development will not only continue, it will pick up as various programs started in the past few years gain traction. In this article we will make some predictions about what we expect in 2021, and we will also supplement it with observations from our partners at Fact Based Insight.

Some General Comments

Other than the technical advances, one of the major changes in 2020 is that some of the hardware developers are getting a lot more transparent about their roadmaps. A major reason for this is because the major vendors want to make potential enterprise clients comfortable enough to invest resources to get started with quantum. These enterprise organizations are not willing to invest in quantum just to get some papers published. They are looking to achieve quantum advantage so their operations can be more efficient and effective and perhaps give them an edge over their competitors.

We have collected dozens of marketing white papers written for end users written by consulting companies, hardware companies, software companies, cloud computing providers and various research labs. They all communicate similar messages with some variation of the following theme:

> Quantum computing technology is advancing at a rapid pace. Although the machines available today may not be quite powerful enough to provide solutions that are intractable for a classical computer, you will see more powerful quantum machines that will be able to provide quantum advantage in the near future. However, utilizing these machines to advantage is not an easy task and you will need to spend time learning which of your problems are best suited for a quantum computer and how to program them to find successful solutions. So we recommend you start now and learning how to do it with toy problems so you will be ready when the more powerful machines are available. And if you don't do it, your competitors invariably will and you will be at a competitive disadvantage in the marketplace. So work with us now and we will show you the way to become quantum ready.

And as a result, we are seeing more and more evidence of various enterprises setting up small group to explore quantum computing applications and we expect this trend to continue.

Key Technical Developments that We Expect to See in 2021

Here are some projections of technical advancements we believe will occur in the coming year.

- Multiple hardware providers will place online a quantum computer with over 100 qubits.
- Quantum computers that are not based on superconducting technology will continue to grow in capabilities and market share. Look for more product introductions of machines based upon photonic, spin qubit, ion traps and cold atom technologies. These can be significant because many of these technologies will not require a dilution refrigerator which will considerably lower the manufacturing cost and physical size of the computer.
- There will be more progress made on hybrid classical/quantum computing to make them work better together. You can expect to see more quantum services implement co-location and have the classical and quantum computer sit next to each other in the same data center to reduce latency delays. There will also be more companies adopting concepts like mid-circuit measurement that will allow branches in a quantum program based upon the outcome of an individual qubit measurement.
- Software improvements will continue to make improvements to make it easier for end users to program and utilize a quantum computer. The number of application libraries will expand and allow an end user to program at a higher and higher level.
- In the meantime, the software layers that take the high level input from the end user and translate it down to optimized gate or pulse level instructions that the qubits can understand will get increasingly sophisticated. Improvements will continue to be made in pulse level control to optimize gate fidelity and compilers that will use intelligent algorithms to reduce gate depth.
- There will be continued advancements in both error mitigation and error correction. The former will be used in NISQ computers to improve gate fidelities and enable circuits with more gates and more gate depth. Although we do not expect fault tolerant quantum computers with full error correction

circuits to be in production in 2021, this research will pave the way for implementing these later this decade.

- There will continue to be a move to make software platforms hardware agnostic so that they can support different quantum computers using different technologies. This will allow end users to create one high level description for their program and then try it on multiple different computers to see which one works the best.
- We expect to see continue expansion in quantum computing cloud offerings. Both Microsoft and Google have been in a beta test mode for their services and we expect them to move to a General Availability mode sometime in 2021. Amazon currently has three hardware platforms running on their Braket service and we expect them to add more hardware partners in the coming years to continue expanding the number of different platforms their customers can choose from. We also expect to see new cloud suppliers coming online in 2021, particular from Europe and Asia.
- One of the limiters to the number of qubits is "**the wiring problem**". If each qubit requires 2 or more coaxial cable wires for control, the physical mechanics of routing hundreds or thousands of these cables from the control electronics at room temperature down to the qubits at millikelvin temperatures become untenable. Intel has introduced a cryo-CMOS chip called Horseridge that can help solve this problem and we expect more advancements here from other players in 2021.
- A major limiter for a quantum internet is the maximum length entangled photons can travel through a fiber optic cable before the signals get too weak to be decoded. The limit with today's technology is, at most, 100 kilometers. It is not possible to use a classical optical repeater because that would violate the No Cloning theorem. Much research is underway for a quantum repeater that could use quantum mechanical principles like entanglement swapping to perform this function, but this would require development of a quantum memory device. Look for breakthroughs in 2021 that will demonstrate advancements in quantum memories that can make quantum repeaters a reality.

Key Quantum Business and Ecosystem Developments that We Expect to See in 2021

Here are some projections of developments we expect to see on the business and ecosystem development side in the coming year.

- We expect that one or more enterprises will announce they have achieved Quantum Advantage and are now using quantum computing in a production mode for solving real world problems.
- The quantum industry will continue to see more partnerships between hardware and software companies and may also see a few acquisitions or mergers. In the long term we expect consolidation in the market. It will take a long time for this to happen, but you may see the first signs of this in 2021.
- In 2020, several governments announced national plans to invest in quantum and make their countries the leader in this technology. We expect this trend to continue with additional countries publishing their national plans and funding objectives so they don't miss out. All the other countries will be looking to see what comes out of China and the U.S. because none of them want those two to get too far ahead.

- One of the limiters in quantum industry growth in 2021 will be the availability of a quantum workforce. This limitation has been recognized and some programs have been initiated in 2020 to help encourage more students to consider a quantum career. These programs will accelerate in 2020 and we expect additional ones to be announced in 2021. One potential area that may prove fruitful will be programs oriented towards classical computing programmers and engineers in mid-career to train them on quantum concepts so they can quickly make meaningful contributions in the quantum industry.

- We do not expect a quantum winter to occur in 2021. We expect the world's economy to start growing again in 2021 as the Covid crisis comes under control. If you believe that every cloud has a silver linings, we will point out that the rapid development of vaccines along with the swift adoption of work-from-home and remote videoconferencing will make everyone more optimistic about technology in general. And the continued successes we expect to see in 2021 will give investors confidence that quantum is not a dead end technology and encourage them to maintain or increase funding.

Supplemental Forecasts from Fact Based Insight

Fact Based Insight has published a series of articles that provide a recap of 2020 and additional prognostications for 2021. Rather than duplicating their efforts, we are providing a link to their articles for readers who want to view additional ideas on what's in store for 2021. The links to these articles are shown below.

- Quantum Hardware Outlook 2021
- Quantum Algorithms Outlook 2021
- Quantum Software Outlook 2021
- Quantum Internet Outlook 2021
- Quantum Timing, Imaging & Sensing Outlook 2021
- Quantum Landscape Outlook 2021

Final Comments

It continues to be critical for those in the quantum industry to manage expectations and minimize the hype. There are a lot of folks in the general public who are intrigued by quantum technology, but do not understand it very well and can easily get the wrong impression. We need to continue to stress that this is a long term effort and just because a new quantum development is announced, it doesn't mean that things change overnight.

One should also recognize that classical computing isn't standing still. Although Moore's Law may be slowing down, the classical computing industry is still making considerable advances in more efficient computer architectures and algorithms. So beating out classical computing will always represent an ever increasing target. One should also remember that quantum computing will never replace classical computing. The two technologies will always work together in much the same way that people use GPU's today as coprocessors to general purpose microprocessors. We do want to thank all of our readers for your support of the Quantum Computing Report and look forward to continue providing you with more insightful news, data and analyses in 2021. And for those of you who are actively working to develop this technology we wish you the best of success in your efforts in the coming year.

23 Dec 2020

7 The Germanium quantum information route

https://www.swissquantumhub.com/the-germanium-quantum-information-route/

In the effort to develop disruptive quantum technologies, germanium is emerging as a versatile material to realize devices capable of encoding, processing and transmitting quantum information.

These devices leverage the special properties of holes in germanium, such as their inherently strong spin-orbit coupling and their ability to host superconducting pairing correlations.

In a paper, scientists has reviewed the Germanium opportunities for quantum technology.

They have started by introducing the physics of holes in low-dimensional germanium structures, providing key insights from a theoretical perspective. They have then examined the materials-science progress underpinning germanium-based planar heterostructures and nanowires. They went on to review the most significant experimental results demonstrating key building blocks for quantum technology, such as an electrically driven universal quantum gate set with spin qubits in quantum dots and superconductor-semiconductor devices for hybrid quantum systems.

We concluded this review by identifying the most promising avenues towards scalable quantum information processing in germanium-based systems.

8 Top 10 cyber security stories of 2020

by Alex Scroxton

https://www.computerweekly.com/news/252493509/Top-10-cyber-security-stories-of-2020

The Covid-19 pandemic fundamentally changed the world of technology in 2020, and the cyber security sector was itself profoundly affected.

But that is not to say a microscopic virus had the headlines all to itself, with developments around data privacy and protection, cloud security, vulnerability and much more, all seizing their share of the spotlight. And as usual, we've not even begun to consider the impact of cyber crime.

Here are Computer Weekly's top 10 cyber security stories of 2020:

(i) **Warning over surge in Zoom security incidents**

Cyber criminals are targeting users of popular videoconferencing application Zoom as millions of office workers turn to collaboration tools to keep in touch with each other during the Covid-19 pandemic.

Check Point's threat research team said it has seen a steady rise in new Zoom domains, with 1,700 created since January, but this has ramped up in the past few days, with 425 new domains registered in the past seven days alone.

Out of these, 70 have now been identified as fake sites, which are impersonating genuine Zoom domains with the intention of capturing and stealing personal information. The numbers reinforce a trend for cyber criminals to take advantage of home working via Zoom, which is used by over 60% of the Fortune 500 and has been downloaded more than 50 million times from the Google Play app store.

(ii) **Broadcom flogs Symantec enterprise security unit to Accenture**

Less than 12 months after acquiring Symantec's enterprise security business for $10.7bn, and barely two months after the deal was completed, Broadcom is selling the security services unit on to Accenture for an undisclosed sum.

Accenture said the deal would make its security unit a leading managed security services provider, enhancing its ability to help organisations "rapidly anticipate, detect and respond to cyber threats".

It will take on a wide-ranging portfolio including global threat monitoring and analysis via a global network of security operation centres, real-time adversary and industry-specific threat intel and incident response.

(iii) **Cosmetics firm Avon faces new cyber security incident**

Avon, the cosmetics brand that suffered an alleged ransomware attack in June 2020, has found itself at the centre of a new and significant security incident after inadvertently leaving a Microsoft Azure server exposed to the public internet without password protection or encryption.

Discovered by Anurag Sen of security tool comparison service SafetyDetectives, the vulnerability meant that anybody who possessed the server's IP address could have accessed an open database of information.

The latest incident comes a little over a month after Avon confirmed a major security incident, although not confirmed to have been a ransomware attack, that took its back-end systems offline and left many of its renowned representatives unable to place any orders.

(iv) **Belgian security researcher hacks Tesla with Raspberry Pi**

Electric automaker Tesla has rolled out an over-the-air patch for its Model X vehicles after being informed of a serious vulnerability in its keyless entry system, identified by Belgian academics, which could have enabled criminals to circumvent the $100,000 car's onboard security systems.

The Tesla Model X's key fob lets its owners automatically unlock their car when approaching it, or by pressing a button, using the Bluetooth Low Energy communications standard to talk to the car via a smartphone app.

This process was bypassed by PhD student Lennert Wouters of the University of Leuven's Computer Security and Industrial Cryptography research group in a proof of concept using a self-made device built from a Raspberry Pi, a modified key fob and engine control unit from a salvaged Model X, and other components costing a total of $195.

(v) **EU moves closer to encryption ban after Austria, France attacks**

The European Union is inching closer to formally ending the use of end-to-end encryption by web platforms such as Signal and WhatsApp, following a spate of Islamist terror attacks in Austria and France.

In a draft resolution document leaked to Austrian TV network ORF, which can be read in full here, the EU said it recognised the value of encryption as a "necessary means of protecting fundamental rights", but at the same time "competent authorities in the area of security and criminal justice" needed to be able to exercise their lawful powers in the course of their work.

Previous European Council conclusions delivered at the beginning of October declared that the bloc planned to "leverage its tools and regulatory powers to help shape global rules and standards", and that funds from its Recovery and Resilience Facility are to be used to enhance the EU's ability to protect against cyber threats, to provide for a secure comms environment – possibly through quantum encryption – and, crucially, "to ensure access to data for judicial and law enforcement processes".

(vi) **Exposed AWS buckets again implicated in multiple data leaks**

The lack of care being taken to correctly configure cloud environments has once again been highlighted by two serious data leaks in the UK caused by misconfigured Amazon Simple Storage Service (S3) bucket storage.

As a default setting, Amazon S3 buckets are private and can only be accessed by individuals who have explicitly been granted access to their contents, so their continued exposure points to the concerning fact that consistent messaging around cloud security policy, implementation and configuration is failing to get through to many IT professionals.

The first leak related to several UK consulting firms. This was uncovered by Noah Rotem and Ran Locar, researchers at vpnMentor, who uncovered information such as passport scans, tax documents, background checks, job applications, expense claims, contracts, emails and salary details relating to thousands of consultants working in the UK.

(vii) **GDPR lawsuit against Oracle and Salesforce moves forward**

The data processing policies and practices of two of the world's largest software companies, Salesforce and Oracle, will come under scrutiny in the High Court of England and Wales in the biggest digital privacy class action lawsuit ever filed.

The suit, filed by privacy campaigner and data protection specialist Rebecca Rumbul, is seeking damages that have been estimated in excess of £10bn, which could conceivably lead to awards of £500 for every internet user in the UK. A parallel suit in the Netherlands backed by a Dutch group called The Privacy Collective Foundation could take the total damages to more than €15bn.

"Enough is enough," said Rumbul. "I am tired of tech giants behaving as if they are above the law. It is time to take a stand and demonstrate that these companies cannot unlawfully and indiscriminately hoover up my personal data with impunity. The internet is not optional any more, and I should be able to use it without big tech tracking me without my consent.

(viii) **Coronavirus: Researcher finds security vulnerability in Slack**

The security risks associated with unified communications and collaboration (UCC) application Zoom have become one of the big stories of the Covid-19 coronavirus pandemic, but other UCC platforms are not immune from problems. According to AT&T's Alien Labs, a vulnerability in cloud-native messaging service Slack could leave meetings open to disruption by malicious actors.

The vulnerability centres on Slack's incoming webhooks, which let users post messages from various applications to Slack. If the user specifies a unique URL, a message body text and a destination channel, they can send a message to any webhook that they know the URL of in any workspace, regardless of their membership.

The Slack vulnerability was uncovered by Alien Labs cloud security researcher Ashley Graves, who said that although webhooks are considered a low-risk integration – the user must select a target channel, which reduces the scope of abuse, the webhook URL is secret, and webhooks only accept data, so cannot, on their own, expose data – this is not entirely accurate.

(ix) **Qualcomm chip vulnerability puts millions of phones at risk**

Smartphone devices from the likes of Google, LG, OnePlus, Samsung and Xiaomi are in danger of compromise by cyber criminals after 400 vulnerable code sections were uncovered on Qualcomm's Snapdragon digital signal processor chip, which runs on over 40% of the global Android estate.

The vulnerabilities were uncovered by Check Point, which said that to exploit the vulnerabilities, a malicious actor would merely need to convince their target to install a simple, benign application with no permissions at all.

The vulnerabilities leave affected smartphones at risk of being taken over and used to spy on and track their users, having malware and other malicious code installed and hidden, and even being bricked outright, said Yaniv Balmas, Check Point's head of cyber research.

(x) **Critical SaltStack vulnerability affects thousands of datacentres**

A series of critical vulnerabilities in SaltStack's open source Salt remote task and configuration framework will let hackers breeze past authentication and authorisation safeguards to take over thousands of cloud-based servers if left unpatched.

Salt is used in infrastructure, network and security automation solutions and is widely used to maintain datacentres and cloud environments. The framework comprises a "master" server acting as a central repository, with control over "minion" agents that carry out tasks and collect data.

The two vulnerabilities, which are assigned designations CVE-2020-11651 and CVE-2020-11652, were uncovered by F-Secure researchers in March 2020 while working on a client engagement.

22 Dec 2020

9 3 Cybersecurity Measures to Ensure Safety in 2021

by Ademola Alex Adekunbi

https://www.entrepreneur.com/article/361376

As the year comes to an end, cybersecurity continues to remain top-of-mind for business owners around the world. The year marked an increase in the amount of fraud perpetrated against small businesses, but especially small- and medium-sized businesses (SMBs). A report by Interpol from earlier in the year showed that cybercriminals have been expanding their attacks against targets from individuals and small businesses to major corporations, governments and critical infrastructure. As highlighted by Wall Street Journal, ransomware and malware attacks have also been increasing drastically.

There are many factors responsible for the marked increase in cyber fraud and malware attacks this year, but the fact that most people have been and are still working from home is likely to be a major contributor. Unlike at work where it is easy to reach out to the IT staff for guidance on what actions to take should a situation arise, many are simply adopting a DIY attitude, and thus making more mistakes. Also, there have been many disruptions in how businesses operate, thus making it easier for bad actors to convince people to depart from the established protocol. Here are three strategies you can adopt to safeguard your business going forward.

(i) **Keep your systems safe**

Most cyber attacks come in the form of software that is installed on your systems through one form or another, and you can reduce the risks of such attacks dramatically simply by ensuring that you have the proper antivirus software installed and updated. The latter part is particularly important because there are new viruses being developed and sold on the internet every day, and if your antivirus software is not kept up-to-date, it might simply miss a piece of malware.

It is also important to make regular backups of important data and to have strong passwords in place across all of your devices. Sometimes, all it takes for an attacker to gain access is one device used by a staff member deploying a weak password or failing to avail themselves of multi-factor authentication on devices and accounts. Even if your organization is not large enough to have a full-fledged IT department, it's important to coordinate your staff to ensure they are taking the steps necessary to keep your systems secure.

(ii) Internet security training and processes

Although the common perception of hackers is that they sit in front of monitors with long lines of green code running down their screens as they use brute force attacks to force their way into a target network, that is simply not the case in many instances. Today, many cybersecurity attacks come in the form of social engineering using carefully crafted emails and calls designed to trick your staff into granting access to the hackers either by installing malware or giving up credentials on webpages controlled by the hackers.

"Businesses must be aware of social engineering tactics and train all of their staff on how to identify and combat them," says Joseph White, CEO of LookupAmerica. "Something as simple as mandating that staff take the time to cross-check the sender of an email, or whether a phone number has been marked as spam by other users, can significantly reduce the chances of a successful attack. The overarching principle in social-engineering prevention tactics is to get your staff to pause, review and verify requests before responding with any information – no matter how innocuous – since hackers often get seemingly mundane information from multiple sources which, when added up, could expose confidential data.

(iii) Conduct regular audits

As with any other kind of audit, the purpose of cybersecurity audits is to evaluate your records to see if there are any red flags that indicate if any part of your system has been compromised. In addition, the audit should include a review of your administrative processes and staff behavior to see if there is anything that needs to be changed to further secure your systems and prevent compromise in the future. Typically, you would need to hire professionals to do this, but the expense is well worth it to prevent successful cyber attacks.

The scope and frequency of the audits will vary depending on your specific circumstances, with ecommerce websites being at the top of the list because apart from your own financial information, you have access to the financial information of your customers and losing it to hackers could result in serious liability for you. Apart from checking for malware and vulnerabilities generally, key things to look out for include whether your payment systems are PCI-DSS compliant and whether your SSL certificate is current and functional.

10 Quantum Computers Will Speed Up the Internet's Most Important Algorithm

by Jeremy Hsu

https://spectrum.ieee.org/computing/software/quantum-computers-will-speed-up-the-internets-most-important-algorithm

The fast Fourier transform (FFT) is the unsung digital workhorse of modern life. It's a clever mathematical shortcut that makes possible the many signals in our device-connected world. Every minute of every video stream, for instance, entails computing some hundreds of FFTs. The FFT's importance to practically every data-processing application in the digital age explains why some researchers have begun exploring how quantum computing can run the FFT algorithm more efficiently still.

"The fast Fourier transform is an important algorithm that's had lots of applications in the classical world," says Ian Walmsley, physicist at Imperial College London. "It also has many applications in the quantum domain. [So] it's important to figure out effective ways to be able to implement it."

The first proposed killer app for quantum computers – finding a number's prime factors – was discovered by mathematician Peter Shor at AT&T Bell Laboratories in 1994. Shor's algorithm scales up its factorization of numbers more efficiently and rapidly than any classical computer anyone could ever design. And at the heart of Shor's phenomenal quantum engine is a subroutine called – you guessed it – the quantum Fourier transform (QFT).

Here is where the terminology gets a little out of hand. There is the QFT at the center of Shor's algorithm, and then there is the QFFT – the quantum fast Fourier transform. They represent different computations that produce different results, although both are based on the same core mathematical concept, known as the discrete Fourier transform.

The QFT is poised to find technological applications first, though neither appears destined to become the new FFT. Instead, QFT and QFFT seem more likely to power a new generation of quantum applications.

The quantum circuit for QFFT is just one part of a much bigger puzzle that, once complete, will lay the foundation for future quantum algorithms, according to researchers at the Tokyo University of Science. The QFFT algorithm would process a single stream of data at the same speed as a classical FFT. However, the QFFT's strength comes not from processing a single stream of data on its own but rather multiple data streams at once. The quantum paradox that makes this possible, called superposition, allows a single group of quantum bits (qubits) to encode multiple states of information simultaneously. So, by representing multiple streams of data, the QFFT appears poised to deliver faster performance and to enable power-saving information processing.

The Tokyo researchers' quantum-circuit design uses qubits efficiently without producing so-called garbage bits, which can interfere with quantum computations. One of their next big steps involves developing quantum random-access memory for preprocessing large amounts of data. They laid out their QFFT blueprints in a recent issue of the journal Quantum Information Processing.

"QFFT and our arithmetic operations in the paper demonstrate their power only when used as subroutines in combination with other parts," says Ryo Asaka, a physics graduate student at Tokyo University of Science and lead author on the study.

Greg Kuperberg, a mathematician at the University of California, Davis, says the Japanese group's work provides a scaffolding for future quantum algorithms. However, he adds, “it’s not destined by itself to be a magical solution to anything. It’s trundling out the equipment for somebody else’s magic show.”

It is also unclear how well the proposed QFFT would perform when running on a quantum computer under real-world constraints, says Imperial’s Walmsley. But he suggested it might benefit from running on one kind of quantum computer versus another (for example, a magneto-optical trap versus nitrogen vacancies in diamond) and could eventually become a specialized coprocessor in a quantum-classical hybrid computing system.

University of Warsaw physicist Magdalena Stobińska, a main coordinator for the European Commission’s AppQInfo project – which will train young researchers in quantum information processing starting in 2021 – notes that one main topic involves developing new quantum algorithms such as the QFFT.

“The real value of this work lies in proposing a different data encoding for computing the [FFT] on quantum hardware,” she says, “and showing that such out-of-box thinking can lead to new classes of quantum algorithms.”

11 What Public And Private Sector Leaders Can Do To Stop The Next SolarWinds Hack

by Gordon Bitko

https://www.forbes.com/sites/gordonbitko/2020/12/22/what-public-and-private-sector-leaders-can-do-to-stop-the-next-solarwinds-hack/?ss=cio-network&sh=22277f3c3814

Americans are only beginning to understand the nature of what is likely to be the worst cyber incident in U.S. government history. Since at least March 2020, malicious code injected into **SolarWinds** products by a nation-state adversary has malignantly infiltrated U.S. networks, inflicting profound, widespread and long-lasting consequences with implications for U.S. government and private sector businesses. The intrusion demonstrates how one operation can impact nearly every sector of the economy and national security, and painfully reminds us that more such attacks are inevitable.

SolarWinds Orion software allows IT administrators to orchestrate every aspect of an organization’s networked functions and services. The tool can access and modify any device or service, and the hackers likely obtained a backdoor across entire networks. With that access, they may have engaged in malicious activities such as observing and compromising operational activity, and modifying or exfiltrating sensitive data.

In order to gain such extensive access, the malware in this attack came from a trusted source, SolarWinds’ own software deployment servers, thus preventing security compliance programs and tools that rely on adversary signatures from blocking the hacker’s activities or alerting network defenders.

While the immediate challenges following the breach are to identify compromised systems, patch vulnerabilities and hunt out bad actors, the long-term struggle is to match adversary persistence with a continuous and more robust investment in improving U.S. security capabilities and expertise.

Having seen similar attacks targeting both the public and private sector while at the FBI, I know that detecting and stopping hackers’ access to trusted sources and credentials is crucial to reducing future breaches. While not a panacea, truly risk-based cybersecurity and supply chain mitigations implemented through public and private sector cooperation can impede even the most sophisticated intruders.

Unfortunately, many of the U.S. government's cybersecurity tools are too reactive to defend against sophisticated incoming attacks. Traditional monitoring and intrusion detection capabilities, such as Cybersecurity and Infrastructure Security Agency's (CISA) Einstein system, are not equipped to catch a high-level threat actor who designed attacks specifically to evade those obstacles. Investing in modern cyber defenses such as zero trust networks is essential and makes an intruder's work harder. This must be coupled with defensive cybersecurity capabilities powered by continuously vigilant human expertise.

The SolarWinds Orion attack was detected by the private sector, and the quick engagement of government reaffirms that a robust public-private sector partnership is fundamental to digital security.

The challenge now is not only closing the door but finding who got into the house and how much damage was done. The human-centric response and recovery to this intrusion will strain limited cybersecurity resources because the government has underinvested in defensive cybersecurity and supply chain management for years. Consequently, not enough skilled professionals are available to perform critical activities in a moment of need. To optimize effectiveness, federal agencies and other potential victims – including industry – will need to expand information sharing, moving beyond the indicators of compromise and common behaviors that led to the initial discovery. This will expedite investigative work by threat hunters and assist in developing automated capabilities to help stop this and future attacks.

Federal agencies' cybersecurity teams must embrace risk-based policies and decisions and may need to limit basic functions to fully learn what critical data and capabilities might have been exposed to the hacker's malicious actions. In the worst-case scenario, it may be more effective and timely to entirely replace high risk systems and networks.

With that information, coupled with an understanding of an organization's critical data and capabilities, victims in both the public and private sector can build upon the risk-based approach of the NIST Cybersecurity Framework, which provides a roadmap for cybersecurity professionals to identify, protect, detect, respond and recover from a breach. Organizations that leverage the current framework in the design of their information security strategies will be better situated to respond to this incident and will be better prepared for inevitable future attacks with a thorough understanding of their digital footprint.

Finally, having designated leadership learn from this incident and implement a plan to address this top national security threat is paramount. The U.S. Congress created and recently approved the position of National Cybersecurity Director for this reason. President Trump should sign this critical position into law without further delay.

President-elect Biden has announced that cybersecurity will be a top priority. His administration should follow through on this promise with investments that balance offensive and defensive cybersecurity, and with a commitment to ensure public and private partners work together in staying ahead of this evolving threat.

21 Dec 2020

12 Artificial intelligence solves Schrödinger's equation

by Freie Universitaet Berlin

https://phys.org/news/2020-12-artificial-intelligence-schrdinger-equation.html

A team of scientists at Freie Universität Berlin has developed an artificial intelligence (AI) method for calculating the ground state of the Schrödinger equation in quantum chemistry. The goal of quantum chemistry is to predict chemical and physical properties of molecules based solely on the arrangement of their atoms in space, avoiding the need for resource-intensive and time-consuming laboratory experiments. In principle, this can be achieved by solving the Schrödinger equation, but in practice this is extremely difficult.

Up to now, it has been impossible to find an exact solution for arbitrary molecules that can be efficiently computed. But the team at Freie Universität has developed a deep learning method that can achieve an unprecedented combination of accuracy and computational efficiency. AI has transformed many technological and scientific areas, from computer vision to materials science. "We believe that our approach may significantly impact the future of quantum chemistry," says Professor Frank Noé, who led the team effort. The results were published in the reputed journal Nature Chemistry.

Central to both quantum chemistry and the Schrödinger equation is the wave function – a mathematical object that completely specifies the behavior of the electrons in a molecule. The wave function is a high-dimensional entity, and it is therefore extremely difficult to capture all the nuances that encode how the individual electrons affect each other. Many methods of quantum chemistry in fact give up on expressing the wave function altogether, instead attempting only to determine the energy of a given molecule. This however requires approximations to be made, limiting the prediction quality of such methods.

Other methods represent the wave function with the use of an immense number of simple mathematical building blocks, but such methods are so complex that they are impossible to put into practice for more than a mere handful of atoms. "Escaping the usual trade-off between accuracy and computational cost is the highest achievement in quantum chemistry," explains Dr. Jan Hermann of Freie Universität Berlin, who designed the key features of the method in the study. "As yet, the most popular such outlier is the extremely cost-effective density functional theory. We believe that deep 'Quantum Monte Carlo,' the approach we are proposing, could be equally, if not more successful. It offers unprecedented accuracy at a still acceptable computational cost."

The deep neural network designed by Professor Noé's team is a new way of representing the wave functions of electrons. "Instead of the standard approach of composing the wave function from relatively simple mathematical components, we designed an artificial neural network capable of learning the complex patterns of how electrons are located around the nuclei," Noé explains. "One peculiar feature of electronic wave functions is their antisymmetry. When two electrons are exchanged, the wave function must change its sign. We had to build this property into the neural network architecture for the approach to work," adds Hermann. This feature, known as 'Pauli's exclusion principle,' is why the authors called their method 'PauliNet.'

Besides the Pauli exclusion principle, electronic wave functions also have other fundamental physical properties, and much of the innovative success of PauliNet is that it integrates these properties into the deep neural network, rather than letting deep learning figure them out by just observing the data. "Building the fundamental physics into the AI is essential for its ability to make meaningful predictions in the field," says Noé. "This is really where scientists can make a substantial contribution to AI, and exactly what my group is focused on."

There are still many challenges to overcome before Hermann and Noé's method is ready for industrial application. "This is still fundamental research," the authors agree, "but it is a fresh approach to an age-old problem in the molecular and material sciences, and we are excited about the possibilities it opens up."

13 Why Quantum Computing's Future Lies in the Cloud

by John Edwards

https://www.informationweek.com/cloud/why-quantum-computings-future-lies-in-the-cloud/a/d-id/1339610?

As cloud providers search for new markets, many are turning their attention to quantum computing, a science that's long been touted as the ultimate disruptive technology, but which is currently limited to a handful of select niches, such as academic research, cryptography, and blockchain.

While quantum computing adopters are currently few and far between, many observers believe that it's only a matter of time before the technology gains the momentum necessary to become commercially viable. That's why cloud providers are now beginning to position themselves to tap into what could eventually turn out to be a very lucrative market.

Quantum and the cloud

Quantum computing's high cost and deep complexity will likely drive most applications off premises and into the arms of cloud providers like Amazon, Google, and Microsoft. While the major cloud players all have extremely deep pockets, most early adopters, such as startups and research labs, aren't particularly well heeled. Even enterprises that can afford to deploy their own quantum systems may wish to spare themselves the time and effort needed to place the technology on premises.

The quantum computers available today are far from "plug and play" systems, observed Celia Merzbacher, deputy director of SRI International's Quantum Economic Development Consortium, a collection of stakeholders dedicated to building and supporting the emerging quantum industry. "It's not practical to install and maintain current quantum computers on premises," she stated, noting that quantum computers are still in development, generally sensitive to the local environment, and require highly trained technical experts to keep them operational.

The current generation of Noisy Intermediate-Scale Quantum (NISQ) computers are large, temperamental, and complicated to maintain, said Konstantinos Karagiannis, an associate director at business, finance, and technology consulting firm Protiviti. They are also very expensive and likely to be rapidly outdated, he added.

Karagiannis, like most other sector experts, believes that the enterprise path to quantum computing access is more likely to go through the cloud than the data center. "Providing cloud access to quantum computers . . . allows researchers and companies worldwide to share these systems and contribute to both academia and industry," he said. "As more powerful systems come online, the cloud approach is likely to become a significant revenue source [for service providers], with users paying for access to NISQ systems that can solve real-world problems."

The limited lifespans of rapidly advancing quantum computing systems also favors cloud providers. "Developers are still early along in hardware development, so there's little incentive for a user to buy hardware that will soon be made obsolete," explained Lewie Roberts, a senior researcher at Lux Research. "This is also part of why so many large cloud players . . . are researching quantum computing," Roberts noted. "It would nicely augment their existing cloud services," he added.

Flexibility is another factor favoring the cloud. "For the foreseeable future, quantum computers will not be portable," observed Jake Farinholt, lead scientist at management and IT consulting form Booz Allen

Hamilton. “Cloud can provide users with access to multiple different devices, as well as simulators, right from their laptops.”

Quantum system support is another headache that most enterprises would prefer to offload to an outside partner. Farinholt points out that quantum computers are extremely fragile, must be maintained at cryogenic temperatures, and require supervision by teams of engineers and physicists. “Cloud infrastructure is the clear choice to provide widespread access at a reasonable price point,” he said.

Potential applications

There’s not going to be a single leading application, Merzbacher predicted. “Just like classical computing, quantum computing will have high-impact applications across many – perhaps even most – aspects of business and daily life,” she noted.

Quantum simulations, in particular, will likely have a major impact on a wide range of enterprises. One example is the pharmaceutical industry. “Many of the challenges in drug discovery boil down to the computational challenges involved in simulating quantum chemistry,” Farinholt said.

In fact, virtually all industries and government organizations stand to benefit from quantum computing. “The Department of Defense spends over $1 billion a year fighting corrosion,” Farinholt observed. “Quantum simulations may enable more rapid discovery and development of novel corrosion-resistant materials, which could drastically reduce costs.” Quantum simulations could also have a massive impact on the environment. He noted, for instance, that quantum technology may lead to the development of more efficient fertilizer production methods, “a process that’s currently responsible for an estimated 1% to 3% of the entire world’s total energy consumption.”

Bob Sutor, vice president of AI, blockchain, and quantum solutions at IBM Research, predicted that chemists may soon turn to quantum computing to create more efficient and longer lasting lithium batteries. “Consumers will see this in electric vehicles, for example,” he said.

Timeframe

Although quantum computing promises an avalanche of research breakthroughs, Kazuhiro Gomi, president and CEO of NTT Research, advised patience. “We expect these applications to become a reality in the next 10 years,” he predicted.

Sutor is more optimistic. “We expect the first quantum advantage applications to come at roughly mid-decade,” he stated. Sutor cautioned, however, that early applications will be isolated and may seem at first more like research experiments than actual commercial applications. “However, the techniques will spread to other industries; they will be improved and new algorithms developed,” he said. “I think we’ll see wave after wave of greatly enhanced quantum applications coming every few years after that.”

14 Connecting Qubits via a Cryogenic Link

by Christopher Crockett

https://physics.aps.org/articles/v13/s162

Powerful quantum computers could be built by linking together multiple superconducting quantum processors. Promising schemes involve exchanging visible or infrared photons through optical fibers and converting such photons into microwave photons that can couple to the superconducting qubits. But the microwave-to-optical transduction can spoil the fidelity of the quantum states. Now, Paul Magnard of the Swiss Federal Institute of Technology (ETH) in Zurich and colleagues have built and tested a link that bypasses the need for frequency conversion[1]. This link directly transfers qubit states encoded in microwave photons from one circuit to another located meters away.

To create their network, the team set up two identical superconducting circuits, each made of a single qubit, and housed them in separate refrigerators about 5 m apart. They connected the refrigerators via an aluminum waveguide, which they nestled in four layers of concentric insulating sleeves arranged like a set of Russian dolls. After cooling the waveguide and the qubits to below 20 mK, the team wrote a quantum state in one qubit, transferred the state across the waveguide, and read it out from the other qubit. Magnard and colleagues showed that they could repeatedly transfer quantum states with high fidelity and also entangle the remote qubits on demand.

The researchers say that their setup could be easily incorporated into a variety of existing communication schemes using microwaves. They also suggest that the link could be stretched to hundreds of meters. In the near term, the team will use this approach to distribute quantum processing tasks between circuits with multiple qubits, which would be an important step in realizing large-scale, modular quantum computing architectures.

15 A massive cyberattack in the US, using a novel set of tools

by Shruti Dhapola

https://indianexpress.com/article/explained/us-solarwinds-hack-cybersecurity-fireeye-russia-7110550/

The '**SolarWinds hack**', a cyberattack recently discovered in the United States, has emerged as one of the biggest ever targeted against the US government, its agencies and several other private companies. In fact, it is likely a global cyberattack.

It was first discovered by US cybersecurity company FireEye, and since then more developments continue to come to light each day. The sheer scale of the cyber-attack remains unknown, although the US Treasury, Department of Homeland Security, Department of Commerce, parts of the Pentagon are all believed to have been impacted.

In an opinion piece written for The New York Times, Thomas P Bossert, who was Homeland Security Adviser for President Donald Trump, has named Russia for the attack. He wrote "evidence in the SolarWinds attack points to the Russian intelligence agency known as the SVR, whose tradecraft is among the most advanced in the world." The Kremlin has denied its involvement.

So, what is this 'SolarWinds hack'?

News of the cyberattack technically first broke on December 8, when FireEye put out a blog detecting an attack on its systems. The firm helps with security management of several big private companies and federal government agencies.

[1] P. Magnard et al., "Microwave quantum link between superconducting circuits housed in spatially separated cryogenic systems," Phys. Rev. Lett. 125, 260502 (2020).

FireEye CEO Kevin Mandia wrote in a blogpost saying that the company was “attacked by a highly sophisticated threat actor”, calling it a state-sponsored attack, although it did not name Russia. It said the attack was carried out by a nation “with top-tier offensive capabilities”, and “the attacker primarily sought information related to certain government customers.” It also said the methods used by the attackers were novel.

Then on December 13 FireEye said cyberattack, which it named Campaign UNC2452, was not lmited to the company but had targeted various “public and private organisations around the world”. The campaign likely began in “March 2020 and has been ongoing for months”, the post said. Worse, the extent of data stolen or compromised is still unknown, given the scale of the attack is still being discovered. After systems were compromised, “lateral movement and data theft” took place.

How did so many US government agencies and companies get attacked?

This is being called a ‘Supply Chain’ attack: Instead of directly attacking the federal government or a private organisation’s network, the hackers target a third-party vendor, which supplies software to them. In this case, the target was an IT management software called Orion, supplied by the Texas-based company SolarWinds.

Orion has been a dominant software from SolarWinds with clients, which include over 33,000 companies. SolarWinds says 18,000 of its clients have been impacted. Incidentally, the company has deleted the list of clients from its official websites.

According to the page, which has also been scrubbed from Google’s Web Archives, the list includes 425 companies in Fortune 500, the top 10 telecom operators in the US. A New York Times report said parts of the Pentagon, Centers for Disease Control and Prevention, the State Department, the Justice Department, and others, were all impacted.

Microsoft confirmed it has found evidence of the malware on their systems, although it added there was no evidence of “access to production services or customer data”, or that its “systems were used to attack others”. Microsoft president Brad Smith said that the company has begun to “notify more than 40 customers that the attackers targeted more precisely and compromised”.

A Reuters report said that even emails sent by Department of Homeland Security officials were “monitored by the hackers”.

How did they gain access?

According to FireEye, the hackers gained “access to victims via trojanized updates to SolarWinds’ Orion IT monitoring and management software”. Basically, a software update was exploited to install the ‘Sunburst’ malware into Orion, which was then installed by more than 17,000 customers.

FireEye says the attackers relied on “multiple techniques” to avoid being detected and “obscure their activity”. The malware was capable of accessing the system files. What worked in the malware’s favour was it was able to “blend in with legitimate SolarWinds activity”, according to FireEye.

Once installed, the malware gave a backdoor entry to the hackers to the systems and networks of SolarWinds’ customers. More importantly, the malware was also able to thwart tools such as anti-virus that could detect it.

Where does Russia come in?

In his NYT opinion article, Bossert named Russia and its agency SVR, which has the capabilities to execute the attack of such ingenuity and scale.

Microsoft notes in its blog that “this aspect of the attack created a supply chain vulnerability of nearly global importance, reaching many major national capitals outside Russia”. It goes on to add that sophisticated attacks from Russia have become common.

FireEye, however, has not yet named Russia as being responsible and said it is an ongoing investigation with the FBI, Microsoft, and other key partners who are not named.

What has SolarWinds and the US government said about the hack?

Right now, SolarWinds is recommending that all customers immediately update the existing Orion platform, which has a patch for this malware. “If attacker activity is discovered in an environment, we recommend conducting a comprehensive investigation and designing and executing a remediation strategy driven by the investigative findings and details of the impacted environment,” it has said.

Those unable to update are told to isolate “SolarWinds servers” and it should “include blocking all Internet egress from SolarWinds servers”. The bare minimum suggestion is the “changing passwords for accounts that have access to SolarWinds servers / infrastructure”.

The US Cybersecurity and Infrastructure Security Agency (CISA) has issued an Emergency Directive 21-01, asking all “federal civilian agencies to review their networks” for indicators of compromise. It has asked them to “disconnect or power down SolarWinds Orion products immediately”.

The FBI, CISA and office of the Director of National Intelligence issued a joint statement, and announced what is called the ‘Cyber Unified Coordination Group (UCG)” in order to coordinate government response to the crisis. The statement calls this a “significant and ongoing cybersecurity campaign.”

The White House and President Donald Trump have been silent. Senator Mitt Romney has summed it best in his comments to journalist Olivier Knox of SiriusXM radio, where he compared this attack to the equivalent of Russian bombers flying undetected all over the country exposing the cyber warfare weakness of the US. He said that the silence and inaction from White House was inexcusable.

Senator Richard Blumenthal, a Democrat, tweeted: “Russia’s cyber-attack left me deeply alarmed, in fact downright scared.”

President-elect Joe Biden said in a statement: “A good defense isn’t enough; We need to disrupt and deter our adversaries from undertaking significant cyber attacks in the first place.”

18 Dec 2020

16 Researchers Achieve First “Sustained” Long Distance Quantum Teleportation

by VICTOR TANGERMANN

https://futurism.com/researchers-achieve-first-sustained-long-distance-quantum-teleportation

A team of researchers claim to have achieved sustained, long-distance quantum teleportation for the first time.

The research could lay the groundwork for “a viable quantum internet – a network in which information stored in qubits is shared over long distances through entanglement” that could “transform the fields of data storage, precision sensing and computing,” according to a Fermilab statement.

The team – a collaboration between the U.S. Department of Energy’s Fermilab, the University of Calgary, and other partners – managed to teleport qubits of photons over 44 kilometers of fiber.

The process doesn’t actually involve teleportation in the traditional sense. Quantum teleportation is the transfer of quantum states from one location to another. Through quantum entanglement, two particles in separate locations are connected by an invisible force, famously referred to as “spooky action at a distance” by Albert Einstein.

Regardless of the distance, the encoded information shared by the “entangled” pair of particles can be passed between them.

By sharing these quantum qubits, the basic units of quantum computing, researchers are hoping to create networks of quantum computers that can share information at blazing-fast speeds.

“This is an advancement towards a more readily available scaling up of such systems in different locations, to build a bigger system,” Christoph Simon, professor of physics at the University of Calgary and co-author of the accompanying study published in the Physical Review journal earlier this month, said in the university’s statement about the research.

But keeping this information flow stable over long distances has proven extremely difficult. The previous world record was held by researchers at the University of Calgary, covering a distance of just six kilometers, as VICE reports.

Researchers are now hoping to scale up such a system, using both entanglement to send information and quantum memory to store it as well.

17 Dec 2020

17 Developing A Unified Crypto Strategy to Get Ahead Of Tomorrow’s Security Threats

https://www.informationsecuritybuzz.com/articles/developing-a-unified-crypto-strategy-to-get-ahead-of-tomorrows-security-threats/

As the security landscape continues to shift our security defenses must evolve too. Traditional and static systems are inherently insecure and become less secure every day; the same is true for cryptography.

Developed centuries ago, cryptography is perhaps one of the earliest security defenses. The application of cryptography for government secrets protection has evolved through wars and global innovation. Today, cryptography is used to protect many of the routine activities we take for granted, like bank transactions and online shopping.

In business environments, cryptography is used to protect and authenticate applications and IoT devices, however the onset of quantum computing means that today’s cryptographic algorithms will become ineffective and obsolete. Our reliance on hardware and software in traditional IT environments and IoT ecosystems makes the potential fallout from broken cryptographic algorithms highly concerning.

Cryptography is an effective defense against cybercriminals targeting devices and systems, however evolving computing power will ultimately erode cryptography's defenses. Many active and deployed IoT devices have lifespans that will exceed the effectiveness of the cryptographic keys assigned to them, making crypto-agility more critical for risk management and mitigation.

Swapping out encryption keys, upgrading crypto libraries or re-issuing digital identities is common practice in response to a critical security threat, but new and emerging threats are generating new consequences that can lead to business disruption or worse, a significant breach event.

Here are 5 increasingly common examples of cryptographic key risk:

- **Compromise or breach of root** – When a Root of Trust (RoT) is breached, all trust is lost. In the case of a certificate authority issuing certificates, a breach renders the chain of trust and all public and private keypairs moot, or even dangerous, as they can be issued and used maliciously. The immediate replacement of that RoT is required, along with the updating of all certificates and keys used by devices.
- **Algorithm depreciation** – Similar to a compromised RoT, a complete replacement is required in the event of algorithm depreciation. Any keys using the affected algorithm are insecure, raising the risk of rogue actors breaking encryption and rendering communication insecure while making data readily accessible.
- **Crypto library bug** – Discovery of a bug inside crypto libraries may require the generation of new keys and certificate reissuance according to the technology used in patching or replacing it.
- **Quantum computing** – According to Gartner analysts Mark Horvath and David Anthony Mahdi, most public-key algorithms in use today will be susceptible to attack by quantum computing processors within the next five to eight years.
- **Certificate expiration** – Certificate expiration is an important mechanism to ensure certificates are regularly refreshed. It offers a check and balance system, in the form of workflow and approvals, to verify authenticity and integrity. With the shift to one-year SSL/TLS certificate lifespans introduced in 2020, the need for automated renewal has reached an all-time high.

Crypto-Agility is Key to Mitigating Cryptography Risk

The greatest challenge in crypto management is that cryptography exists everywhere – it's diverse, hidden and divided across services, PCs, firewalls and devices. Having a strategy and automated tools that permit agility and the ability to change out algorithms is essential. When developing or augmenting a business' crypto strategy, the following seven steps can help IT teams get ahead of potential disruptions, respond to high-level crypto risk, strengthen cryptographic defense and act before threats become serious:

(i) Conduct an audit to understand how many digital certificates the organization has.

(ii) Build an inventory to identify where they live and what they're used for.

(iii) Document the hash algorithm they use and their overall health.

(iv) Flag certificate expiration dates.

(v) Assign or note who owns every certificate.

(vi) Map the methods used to protect valuable code-signing certificates.

(vii) Ensure a centralized method is used to securely update every certificate.

Many experts believe that quantum computing will pose a legitimate threat somewhere between 2025 and 2035. When it does, today's cryptographic algorithms such as RSA and ECC will become easily breakable. While 2025 may seem like a long way off, many systems being designed and deployed today will still be around then – especially "long-life" cryptographic systems such as industrial-focused IoT devices, cryptocurrencies, and Public Key Infrastructure (PKI), making the practice of cryptography paramount to getting it right.

18 IBM launches experimental homomorphic data encryption environment for the enterprise

by Charlie Osborne

https://www.zdnet.com/google-amp/article/ibm-launches-experimental-homomorphic-data-encryption-environment-for-the-enterprise/

IBM has launched a fully homomorphic encryption (FHE) test service for the enterprise in the first step to bringing in-transit encrypted data analysis into the commercial sector.

IBM said on Thursday that the new FHE solution, IBM Security Homomorphic Encryption Services, will allow clients to start experimenting with how the technology could be implemented to enhance the privacy of their existing IT architecture, products, and data.

FHE, considered by some as the "Holy Grail" of encryption, as it is a form of encryption that allows data to remain encrypted when being processed.

The concept behind FHE is to plug the gap between securely-encrypted data held in storage and the need to decrypt while this information is in use – a requirement in data processing or analysis – which can create protection issues.

While IBM and others in the research community have been working on developing homomorphic encryption for over a decade, FHE has not been considered practical, due to the high compute power required to work with encrypted data, as well as the sluggish speeds of computations.

Now, however, IBM says that due to increases in industry compute power and the refinement of algorithms behind FHE, calculations can now be performed in seconds per bit, "making it fast enough for many types of real-world use cases and early trials with businesses."

IBM is also working on making FHE "quantum-safe" by implementing lattice cryptography.

The company has completed a number of field trials and clients have been working on pilot programs this year to implement FHE. Available now, customers can access an IBM Cloud testing environment to create prototype applications utilizing FHE, and IBM trainers will be on hand to support new FHE projects.

IBM Research tools will also be made available for specific use case tests, including encrypted search and machine learning (ML) features.

"Fully homomorphic encryption holds tremendous potential for the future of privacy and cloud computing, but businesses must begin learning about and experimenting with FHE before they can take full advantage of what it has to offer," commented Sridhar Muppidi, IBM Security CTO.

The technology is still in its early stages and is yet to reach commercial maturity, but by offering a test environment, IBM may be able to resolve FHE implementation and performance challenges, and as such, the company says that the initial offering is focused on developers and engineers in the cryptographic space.

16 Dec 2020

19 Researchers Make Quantum Material Using 53-Qubit IBM Quantum Processor and Qiskit

by Ryan F. Mandelbaum

https://medium.com/qiskit/researchers-make-quantum-material-using-53-qubit-ibm-quantum-processor-and-qiskit-aa63c9c64dc

A team at the University of Chicago made a quantum material called an exciton condensate using a 53-qubit IBM Quantum Hummingbird processor according to a new paper, demonstrating an exciting use for near-term quantum devices for physicists.

Condensates form when a collection of atoms or particles collapse into the same quantum state, so that quantum mechanical phenomena usually restricted to single particles can now describe the entire system. Though you're probably most familiar with Bose-Einstein Condensates, condensates can also form from excitons, bound states of charged particles plus holes with the opposite charge, where holes are simply discrete locations in the medium that have charge due to the lack of an expected particle. The team not only succeeded in generating one of these exciton condensates on a superconducting quantum computer, but uncovered a new behavior of these materials as they formed groups of smaller condensates. This experiment demonstrates the potential power of a quantum computers to pursue problems at the forefront of physics – even today, on noisy quantum devices.

"The noise is what taught us something new," said David Mazziotti, professor in the department of chemistry at the University of Chicago.

First predicted fifty years ago, exciton condensates are superfluids – the particle-hole pairs flow without losing any energy through friction. These superfluid properties could one day be useful for designing new wires or other more energy-efficient devices. Physicists have only recently produced these exciton condensates, and only in certain systems, like in two stacked layers of single-carbon-thick graphene sheets in a magnetic field.

Graphene bilayers are a challenging system in which to produce exciton condensates, so the University of Chicago team turned to the transmon qubits at the core of superconducting quantum computers to control the excitons. Transmons are devices where electric current oscillates near absolute zero, and the lowest two modes of the oscillation represent the zero and one state used for computation. But since these oscillators follow the rules of quantum mechanics, they can oscillate in the zero and one state simultaneously, or their oscillations can become correlated with other transmons' oscillations. The exciton particle-hole pairing behavior acts analogously to the behavior of those transmon qubits interacting with microwave photons, and follows the same rules, giving the team a way to create a system that behaves exactly like an exciton condensate – and a way to control it.

“We have really created something that can be interpreted as an exciton condensate of photon-hole pairs,” said Mazziotti.

The team used the 53-qubit IBM Quantum Hummingbird r1 system to generate the quantum state of the condensate, first with 3 qubits (or excitons) and then with all 53 qubits. First, they applied a Hadamard gate (the superposition gate) to qubit 0, then a CNOT gate (the entangling gate) between qubits 0 and 1, 1 and 2, etc., creating the extremely entangled Greenberger–Horne–Zeilinger, or GHZ state. They looked for the signature of an exciton condensate via a large eigenvalue of the density matrix that describes the system, modified to remove other known effects that may also result in a large eigenvalue. When they calculated this modified density matrix for the system on the quantum computer, the found the telltale sign: an eigenvalue larger than 1.

As the state formed, the researchers were able to observe something not observed before: the effect of noise on a large exciton condensate. The condensate broke up into “islands of condensation,” or smaller units of exciton condensate, before dissipating completely, said LeeAnn Sager, the study’s first author and graduate student in Mazziotti’s group,

“The islands of condensation were something that neither David or I could have predicted,” said Sager. “You never know what’s going to happen with a system as you scale up larger and larger. We thought that the error might be too large – but the system was stable enough that we could observe this effect.”

The IBM Quantum team was excited to have offered access and expertise to the 53-qubit processor as part of their Academic Partner Program. “The machines we are building now will lead to powerful computation devices in the future but even now they are extremely valuable scientific instruments,” said Sebastian Hassinger, IBM Q Network Academic Partner Program lead. “Our academic partner program exists to help researchers conduct new experiments that can produce new science.”

Not only did this research demonstrate the benefits of access to early quantum devices, but also the power of an open-source software and software community supporting these systems. On top of the software’s ability to make the necessary calculations, Sager relied on the Qiskit Slack in order to get quick support while troubleshooting issues.

Quantum computers are noisy devices today that don’t have practical applications in general-purpose fields, yet. However, for physicists, even today’s computers represent the largest and most complex tests of quantum mechanics. This exciton condensate experiment demonstrates that even noisy quantum devices can be useful for those working on the forefront of physics.

“This is a great example of a creative application using our 53-qubit device,” said Jamie Garcia, Senior Manager of Quantum Applications, Algorithms, and Theory on the IBM Quantum Team. “Consistent with what we have seen in our own research, testing hypotheses on the hardware can lead to unexpected and exciting scientific results. These observations can then, in turn, inform future studies and lead to innovations in quantum computing.”

20 The IBM Quantum Challenge Fall 2020 results are in

by Yuri Kobayashi

https://www.ibm.com/blogs/research/2020/12/quantum-challenge-fall-results/

What does programming for the not-so-distant quantum future look like?

From November 9 to 30, more than 3,300 people from 85 countries applied for the 2,000 seats of the IBM Quantum Challenge to find out.

As our cloud-accessible quantum systems continue to advance in scale and capability with better processors of larger number of qubits, understanding how to implement complex data structures become crucial to us in order to harness the potential of our future quantum systems.

During the three-week challenge, participants learned how to implement complex quantum data structures using qRAM and design a quantum game solver using Grover's algorithm. The combination of qRAM and Grover's algorithm has many practical applications in solving real-life problems on our future quantum systems in areas of quantum machine learning and complex decision making problems.

Participants were presented with a new set of exercises each Monday during the challenge, which became progressively more difficult each week. Of the 2,000 participants, 1,091 were able to solve at least one of the first week's exercises, 576 were able to solve at least one of the second week's exercises, and 227 were able to successfully solve all of the exercises, including the final, most-challenging exercise!

Read an example solution, written by the author of the final exercise, IBM Quantum's Atsushi Matsuo, here.

Meet the top 10 scorers of the Quantum Challenge

Our winner, who was not only one of the 227 who completed all of the exercises, but also achieved the lowest quantum cost in solving the final exercise is University of Tokyo undergraduate student, Hironari Nagayoshi. He achieved the lowest quantum cost by applying a strategy based on exploiting the unique traits of the problem's constraints. You can find his solution, here. (link directly to Hironari's solution notebook) which includes commentary on his approach and strategy. Very impressive. Congratulations Hironari!

We were amazed by the ingenuity and creativity of the scorers who came up with brilliant solutions to the final exercise. As one of our participants described in his tweet, one of the best things from the IBM Quantum Challenge is the special opportunity to see how beautifully others think. Please check out the beautiful solutions from our top scorers here.

Top ten scorers of the IBM Quantum Challenge Fall 2020

Ranking	Name	Score
1	Hironari Nagayoshi	4,004
2	Adam Szady	4,819
3	Pulkit Sinha	5,124
4	Witold Jarnicki	6,065
5	Lukas Burgholzer	6,552
6	Jan Tulowiecki	6,574
7	Guillermo Alonso	7,799
8	Stefan Hillmich	8,188
9	Joel Sunil	8,864
10	Chris Chen	9,127

Scores were determined by measuring the circuit implementation cost to solve the final exercise. Cost is defined as: Cost = S + 10C, where S is the number of single-qubit gates and C is the number of CNOT (CX) gates. Any given quantum circuit can be decomposed into single-qubit gates and two-qubit gates. With the current Noisy Intermediate-Scale Quantum (NISQ) devices, CNOT error rates are generally ten times higher than a single qubit gate. Therefore, we weigh CNOT gates ten times more than a single-qubit gate for evaluating the circuit implementation cost.

21 Cambridge Quantum Computing Investing in Cybersecurity, Other Near-Term Quantum Solutions

https://insidehpc.com/2020/12/cambridge-quantum-computing-investing-in-cybersecurity-other-near-term-quantum-solutions/#:~:text=Cambridge%20Quantum%20Computing%20Investing%20in%20Cybersecurity%2C%20Other%20Near%2DTerm%20Quantum%20Solutions,-December%2016%2C%202020&text=Last%20week%20the%20company%20announced,according%20to%20independent%20industry%20sources.

Cambridge Quantum Computing (CQC), a specialist in quantum software and quantum algorithms designed to leverage quantum hardware, today announced it will apply much of its recent fundraise on helping clients achieve near-term quantum solutions in their businesses.

Last week the company announced a $45 million financing, the largest private investment ever announced for a quantum software company, according to independent industry sources. Quantum hardware developers IBM and Honeywell joined leading international investment firms in the financing.

With projected gains in quantum computing performance by hardware developers over the next 2-3 years, and with corresponding enhancements in quantum software, Cambridge Quantum believes it can help clients achieve quantum solutions in several key areas during what is known as the Noisy Intermediate-Scale Quantum (NISQ) computing era. These include:

- Using existing quantum computers to provide the best security possible. As part of a joint effort with IBM, CQC launched a beta quantum random number generation (QRNG) service in September initially available to members of the IBM Q Network with applications primarily to protect and defend global communications and electronic assets.
- CQC is working with the UK's National Physical Laboratory to accelerate research and development to support the commercialization and optimization of its quantum technologies. A key focus will be enhancing CQC's IronBridge for the commercial market, a photonic quantum device that ensures device independence and source certifiability of quantum randomness for post-quantum encryption algorithms as well as use cases in science, engineering, finance and gaming. The organizations have committed to an 18-month timeframe for enhanced quantum products for the global market.
- CQC scientists have formerly established that Quantum Natural Language Processing is "quantum-native" with expected near-term advantages over classical computers, enabling "meaning-aware" NLP for the first time. Potential use cases over the next several years are many, including doctors querying the entire medical literature for patient diagnostics.

"Our highly successful financing will enable new possibilities in achieving quantum solutions for clients in several key areas," said Ilyas Khan, CEO of Cambridge Quantum Computing. "Quantum computing is quickly morphing from the research lab into commercialization and we believe our quantum software and algorithms will play a critical role in this rapid transformation."

15 Dec 2020

22 Performance of Variational Quantum Factoring on a superconducting quantum processor

https://www.swissquantumhub.com/performance-of-variational-quantum-factoring-on-a-superconducting-quantum-processor/

Zapata Computing, in collaboration with IBM, has analyzed the performance of Variational Quantum Factoring (VQF) on superconducting quantum processor.

Quantum computers hold promise as accelerators onto which some classically-intractable problems may be offloaded, necessitating hybrid quantum-classical workflows. Understanding how these two computing paradigms can work in tandem is critical for identifying where such workflows could provide an advantage over strictly classical ones.

In their work, they have studied such workflows in the context of quantum optimization, using an implementation of the Variational Quantum Factoring (VQF) algorithm as a prototypical example of QAOA-based quantum optimization algorithms.

They have executed experimental demonstrations using a superconducting quantum processor, and investigate the trade-off between quantum resources (number of qubits and circuit depth) and the probability that a given integer is successfully factored.

In their experiments, the integers 1,099,551,473,989 and 6,557 had been factored with 3 and 5 qubits, respectively, using a QAOA ansatz with up to 8 layers.

These results empirically demonstrate the impact of different noise sources, and reveal a residual ZZ-coupling between qubits as a dominant source of error.

Additionally, they were able to identify the optimal number of circuit layers for a given instance to maximize success probability.

23 THE ROLE OF QUANTUM COMPUTING IN AUTOMOTIVE INDUSTRY

by Priya Dialani

https://www.analyticsinsight.net/the-role-of-quantum-computing-in-automotive-industry/

Quantum computing has gained a lot of footing from both general society and private areas lately. Companies have seen putting gigantic capital into quantum computing research; the most recent few years saw the busiest years for this innovation.

After organizations, for example, IBM with its Q System One or D-Wave Technologies stood out as truly newsworthy lately with probably usable quantum computers, different organizations in the automotive value chain have analyzed this innovation, the promises made by producers were excessively alluring. As indicated by their promises, quantum computers are ideal for taking care of specific issues that the best researchers have for some time been agonizing over, for example, route optimisation, the durability of materials, and fuel cell optimisation.

According to McKinsey, one-tenth of all potential QC use cases under exploration could profit the automotive business. Indeed, automotive will be one of the essential value pools for quantum computing, with a high impact observable by around 2025. Additionally, it is anticipated a critical economic impact of related advances for the automotive business, assessed at $2 billion to $3 billion, by 2030. Most of the early worth added will come from tackling complex optimization issues, including processing huge amounts of information to accelerate learning in autonomous-vehicle-navigation algorithms. In later years, quantum computing can possibly positively affect numerous areas in the automotive business, for example, vehicle directing and course enhancement, material and process research, and the security of connected driving.

Somewhere else, significant investments have just been made, with German provider Bosch procuring a stake in Massachusetts-based quantum start-up Zapata Computing, adding to a US$21 million Series A investment.

BMW, Daimler, and Volkswagen have declared that they are effectively seeking after quantum computing research, including quantum simulation for material sciences, intending to improve the proficiency, safety, and durability of batteries and fuel cells.

Over the long-term, from 2030 ahead, quantum-computing applications will expand on at-scale admittance to universal quantum computers. Prime factorization algorithms to break basic encryption keys will in this manner be universally accessible. The focus will probably push toward digital security and risk mitigation as players attempt to forestall the quantum hacking of communications in autonomous vehicles, on-board hardware, and the Industrial Internet of Things. The cloud-facilitated navigation frameworks of shared-mobility fleets will improve their coverage algorithms through regular training enabled by quantum computing.

Supply routes including a few methods of transport could be streamlined utilizing algorithms created through quantum computing, while different applications will improve energy stockpiling and generative algorithms. Quantum computing could likewise assist providers with improving or refine kinetic properties of materials for lightweight structures and glues, as well as create proficient cooling systems.

Quantum computers will be used via automakers during vehicle design to deliver enhancements identifying with minimizing drag and improving eco-friendliness. Likewise, quantum computers can perform advanced simulations in fields, for example, vehicle crash behavior and lodge soundproofing, just as to train algorithms utilized in the improvement of autonomous-driving software. Quantum computer–s capability to decrease computing times from half a month to a couple of moments implies that OEMs could guarantee vehicle-to-vehicle communications in real-time, every time.

Quantum computing isn't probably going to supplant existing high-performance computing (HPC), however, will rather depend vigorously on hybrid schemes where a traditional HPC can help refine problem-solving more efficiently. A computational issue, for instance, to locate the most effective choice among billions of potential combinations will at first be iterated with a quantum computer to find a surmised solution before the remainder is taken care of by an HPC to adjust evaluations in the subset of solution space.

The pathway for quantum computing is as yet dubious notwithstanding its potential. Putting resources into quantum computing is a substantial responsibility yet will very likely put organizations in front of contenders sometime later whenever it becomes more mainstream in use.

14 Dec 2020

24 Encryption: Council adopts resolution on security through encryption and security despite encryption

https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/#

The Council today adopted a resolution on encryption, highlighting the need for security through encryption and security despite encryption.

In this resolution, the Council underlines its support for the development, implementation and use of strong encryption as a necessary means of protecting fundamental rights and the digital security of citizens, governments, industry and society. At the same time, the Council notes the need to ensure that competent law enforcement and judicial authorities are able to exercise their legal powers, both online and offline, to protect our societies and citizens.

Law enforcement authorities and the judiciary are increasingly dependent on access to electronic evidence to effectively fight terrorism, organised crime, child sexual abuse, and a range of other cybercrime and cyber-enabled crimes. Such access is essential to the success of law enforcement and criminal justice in cyberspace. However, there are instances where encryption renders access to and analysis of evidence extremely challenging or impossible in practice.

The EU is striving to establish an active discussion with the technology industry, and with close involvement from research, academia, industry, civil society and other stakeholders, so as to strike the right balance between ensuring the continued use of strong encryption technology and guaranteeing the powers of law enforcement and the judiciary to operate on the same terms as in the offline world. Potential technical solutions will need to respect privacy and fundamental rights, and preserve the value that technological progress brings to society.

25 Whole-genome sequence data can now be transmitted in real-time by Quantum cryptography

https://www.biospectrumasia.com/news/50/17271/whole-genome-sequence-data-can-now-be-transmitted-in-real-time-by-quantum-cryptography.html

Tohoku University and Toshiba Corporation have achieved a world first, transmitting the whole genome sequence data of 24 people in real-time using quantum cryptography.

The data, which exceeded several hundred gigabytes, had an average key distribution speed greater than 10 megabits per second over standard fiber-optic lines, and arrived at the Tohoku Medical Megabank Organization (ToMMo) just two minutes after Toshiba had finished analyzing it.

The successful experiment demonstrated that quantum encryption technology is now capable of large-capacity data transmission, opening up many practical applications in genomic medicine and research.

Cryptographic protection of sensitive information is increasingly under threat from quantum computers, and researchers have been looking for new ways to protect secret keys used to send and unlock encrypted data. Quantum cryptographic communication technologies apply the principles of quantum mechanics to protect cryptographic communications against wiretapping or decryption. It is often called the "ultimate code" as it is considered impossible to hack.

According to Toshiba, its cryptography technology is hack-proof because it uses light particles, called photons, to send encrypted data and a key for decryption. Attempts to eavesdrop or intercept the data illegally would change the state of the photons, rendering the key unusable.

This technology is expected to be vital for the backup of confidential data and for encrypting transmissions that require a high degree of confidentiality, such as banking and medical data, as well as sensitive information relating to national security. Many countries have been rushing to put quantum cryptography into practical use, and Toshiba hopes to be the first Japanese firm to commercialize the technology.

26 IonQ, QC Ware Researchers Team Up to Tackle Quantum Machine Learning Challenge

by Matt Swayne

https://thequantumdaily.com/2020/12/14/ionq-and-qc-ware-researchers-say-solving-this-quantum-machine-learning-challenge-is-an-important-step-and-could-have-huge-practical

QC Ware and IonQ report they teamed up to run a machine learning algorithm for classification on an 11-qubit quantum qubit.

The experiment is discussed in QC Ware's Medium blog and reported in a paper on arXiv, a pre-print depository.

According to the post, the teams focused on loading classical data onto quantum states in a resilient way to facilitate quantum machine learning – or QML – applications.

Team members reported: "Central to the success of our experiment are QC Ware's own Forge Data Loader™ technology, which optimally transforms classical data onto quantum states, and the high-quality, fully connected qubits of IonQ's 11 qubit system."

According to the researchers, loading classical data onto quantum states is challenging for a number of reasons. First, while most experts assume that QRAM – quantum random access memory – must be available, most proposals require significant hardware investments, qubit count and circuit depth. The team reports that the Forge Data Loader provides a better alternative to QRAM. The technology can load such data points with just 100 qubits and a circuit depth of 100, the researchers added.

The team reports their results: "QC Ware's quantum algorithm running on IonQ's hardware performed at the same level as the corresponding classical algorithm, identifying the right digits 8 out of 10 times on average, the same number of times as the classical algorithm running on classical hardware. This can be seen below in the classical and quantum confusion graphs for the MNIST datasets. This is the first time ever that a classification task with 10 classes has been performed on a quantum computer."

This technology offers several long-term advantages in useful quantum computing, according to the researchers.

First, it takes fewer steps and less time to complete the calculations, meaning processing is faster and better. Second, the team argues that this method is scalable. Accuracy of the algorithm should hold as the problem size increases without the need for error-corrected qubits.

The advance could have the following industry impacts, according to the researchers:

- Opens the way for various quantum machine learning applications, including natural language processing, decision-making, customer recommendations, and fraud detection
- Speeds up the industry timeline for practical QML applications on near-term quantum computers
- Shows the potential for the coming generation of quantum machines to outperform classical computers

12 Dec 2020

27 Toronto Company Focusing on Real-World Quantum Applications Rather Than Far-Fetched Realizations of The Technology

by James Dargan

https://thequantumdaily.com/2020/12/12/toronto-startup-focusing-on-real-world-quantum-applications-rather-than-far-fetched-realizations-of-the-technology/

Temperature, Pressure & Radiation

One of the greatest achievements of science to date has been the molecular-level manipulation of material properties. Nanotechnology, the formal scientific epithet to all this hocus-pocus, has allowed man to improve the controlled delivery of drugs, biocompatible materials, build more advanced sensors, enhance telecommunications tech and delivery, develop state-of-the-art pharmaceutical products, and develop the most indestructible surface coatings the world has ever seen by controlling – somehow – the physical effects of temperature, pressure and radiation.

All breathtaking achievements, but there's still more around the corner to come for the development of nanomaterials and the science of nanotechnology in general.

Smart materials, polymers, nanostructured coatings, composites, and hybrids have yet to reach their full potential in becoming practical appliances useful for our everyday lives. Technologies like nanojoining and nanotribology, though talked about in nanotechnology conferences around the globe as the new messiahs for the advancement of the science, are in their early stages.

Yet the technology will get there, helped along by the sorcery of quantum mechanics.

One company, focused on the development of advanced materials for OLED displays for TVs and the automotive industry with quantum mechanics at play, has some of the things already mentioned in mind.

OTI Lumionics – whose goal is to manipulate quantum computing (QC) for the benefit of materials discovery – was founded in Toronto almost a decade ago now, in 2011. Proud of the fact it's a unique player in the space, OTI's leading-edge OLED solutions are revolutionizing the consumer electronics market with a quantum twist, of course.

28 Zodiac killer code cracked by Australian mathematician Samuel Blake more than 50 years after first murder

by Michael Coggan

https://amp-abc-net-au.cdn.ampproject.org/c/s/amp.abc.net.au/article/12977342

Melbourne mathematician Samuel Blake and two fellow cryptologists have been officially recognised by the United States Federal Bureau of Investigation for solving a 50-year-old cryptic message written by an as yet unnamed serial killer, known only as the Zodiac.

Dr Blake worked on decoding the message known as the "**340 cipher**" with two other cryptologists and a University of Melbourne supercomputer called Spartan to eventually reveal its content.

The cipher bears a distinctive circle with a cross through the middle and was sent to the San Francisco Chronicle newspaper on November 8, 1969 by a man who called himself "Zodiac".

The correspondent killer sent letters to newspapers over several years up until 1974, including proof he was responsible for the deaths of at least five people in the San Francisco Bay Area.

The official cracking of the 340-character cipher provides insight into the killer's thoughts and actions but does not reveal a name as promised in separate letters sent to newspapers.

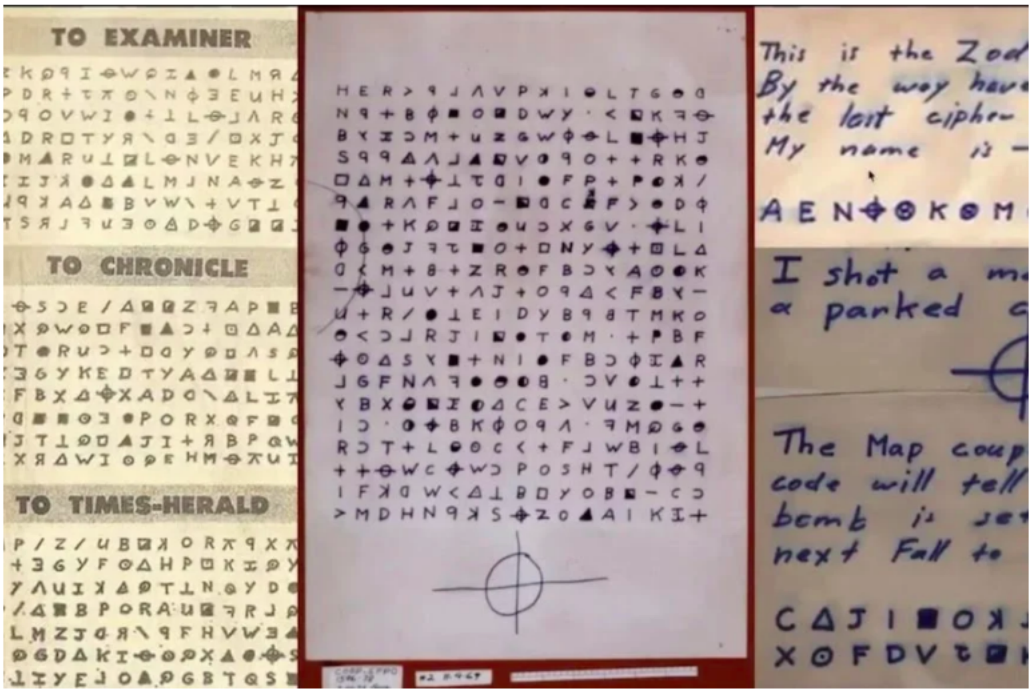


Figure 1: The Zodiac killer sent handwritten codes to local newspapers in the San Francisco Bay Area in the 1960s and 70s.

Dr Blake told the ABC he had been working on finding a solution to the 340 cipher, considered one of the holy grails of cryptography, since contacting Zodiac cryptologist David Oranchak early in 2020.

Mr Oranchak hosts a website dedicated to cracking the Zodiac ciphers and has posted several YouTube videos detailing the work he has done over 15 years trying to solve them.

In a statement released on social media Dr Blake paid tribute to US-based Mr Oranchak and software programmer Jarl van Eycke, based in Brussels.

"During the year we tested, by trial and error, around 650,000 different reading directions through the cipher. This search turned up – more or less – nothing," he said.

"However, one of these searches uncovered a surprising combination of words: GAS CHAMBER. That such a macabre phase should pop up in a sea of noise warranted further attention.

"From this fragment, David, Jarl van Eycke and I reworked the key and corrected an error Zodiac made in his diagonal enumeration of the second vertical segment of the cipher.

"Jarl's fantastic program, azdecrypt, was essential in this process."

A deciphered section of the code

I HOPE YOU ARE HAVING LOTS OF FUN IN TRYING TO CATCH ME

THAT WASN'T ME ON THE TV SHOW

WHICH BRINGS UP A POINT ABOUT ME

I AM NOT AFRAID OF THE GAS CHAMBER

BECAUSE IT WILL SEND ME TO PARADICE ALL THE SOONER

BECAUSE I NOW HAVE ENOUGH SLAVES TO WORK FOR ME

WHERE EVERYONE ELSE HAS NOTHING WHEN THEY REACH PARADICE

SO THEY ARE AFRAID OF DEATH

I AM NOT AFRAID BECAUSE I KNOW THAT MY NEW LIFE IS

LIFE WILL BE AN EASY ONE IN PARADICE DEATH

Dr Blake is a visiting fellow at the University of Melbourne and described how the university's supercomputer, Spartan, solved the cipher after processing 650,000 other possible solutions.

Eventually a solution that drew out a message that included the phrase "GAS CHAMBER" was revealed.

Mr Oranchak sent the proposed solution to the Cryptanalysis and Racketeering Records Unit of the FBI and within a day they officially approved the solution.

In a statement released on Friday, US time, the FBI confirmed that the cipher attributed to the Zodiac Killer was recently solved by "private citizens."

"After 50 years of active research, this cipher has finally been solved. We now understand why it resisted attacks for so long," Dr Blake wrote on social media.

"The reading direction through the cipher was so obscure, that the only way it could be found was with a massive search through many candidates using sophisticated software which can efficiently solve **homophonic substitution ciphers**.

"Not only were we lucky enough to find the needle in the haystack, but we were lucky enough to pick the right haystack in order to start searching for the needle."

Dr Blake and his colleagues have dedicated their work to the murder victims and their families.

The Melbourne mathematician now hopes the solution he and his colleagues have revealed will help crack the two remaining unsolved short ciphers: one with 13 symbols and the other with 32.

In correspondence, the killer hinted that these ciphers contain his name.

“I find the Zodiac case intriguing, but I’m far from a Zodiac killer expert,” Dr Blake said.

“Perhaps my lack of knowledge of the case helped as it wasn’t a distraction.

“It would be fantastic if this helps the investigation in some way, now it’s over to the experts in interpreting the meaning of his message.”

11 Dec 2020

29 How Password Hashing Algorithms Work and Why You Never Ever Write Your Own

by Fletcher Heisler

https://www.veracode.com/blog/secure-development/how-password-hashing-algorithms-work-and-why-you-never-ever-write-your-own

Are you fascinated with cryptography? You’re not alone: a lot of engineers are. Occasionally, some of them decide to go as far as to write their own custom cryptographic hash functions and use them in real-world applications. While understandably enticing, doing so breaks the number 1 rule of the security community: don’t write your own crypto.

How do hashing algorithms work and what’s special about password hashing? What does it take for an algorithm to get ready for widespread production use? Is security through obscurity a good idea? Let’s see.

How does password hashing work?

Before storing a user’s password in your application’s database, you’re supposed to apply a cryptographic hash function to it. (You’re not storing passwords in plain text, right? Good.)

Any cryptographic hash function converts an arbitrary-length input (a.k.a. “message”) into a fixed-length output (a.k.a. “hash”, “message digest”). A secure cryptographic hash function must be:

- **Deterministic:** hashing the same input should always render the same output.
- **One-way:** generating an input message based on a given output should be infeasible.
- **Collision-resistant:** finding two input messages that hash to the same output should also be infeasible.
- **Highly randomized:** a small change in input should lead to a significant and uncorrelated change in output (a.k.a. “the avalanche effect”). Without this property, applying cryptoanalysis methods will allow making predictions about the input based on the output.

Now, there’s general cryptographic hashing, and then there’s password hashing that is somewhat special.

Standard cryptographic hash functions are designed to be fast, and when you're hashing passwords, it becomes a problem. Password hashing must be slow. You want to make it as hard as possible for the attacker to apply brute force attacks to passwords in your database should it ever leak. This is why you want to make passwords hashing computationally expensive. How expensive? Well, it's a tradeoff between convenience for your legitimate users when they validate their passwords and making brute-force attacks hard for the attacker.

To make hashing computationally expensive, a special kind of functions is commonly used: **key derivation functions (KDFs)**. Under the hood, KDFs invoke hashing functions, but they add a random salt before hashing, and then apply numerous (usually thousands or tens of thousands) iterations of hashing. Ideally, they make brute force attacks both CPU-intensive and memory-intensive.

A key derivation function produces a derived key from a base key and other parameters. In a password-based key derivation function, the base key is a password and the other parameters are a salt value and an iteration count (RFC 2898: Password-Based Cryptography Specification Version 2.0).

In password hashing discussions, the terms "hash function" (such as MD5 or SHA-1 or SHA-2 or SHA-3) and "key derivation function" (such as PBKDF2 or Argon2) are often used interchangeably although they're technically not the same.

Why shouldn't you write your own password hashing algorithm?

Both writing a custom hashing algorithm and creating your own implementation of a well-known algorithm are bad ideas. Why?

You probably don't have the skills. Let's face it: cryptography is hard, and messing up an algorithm or implementation is easy, even for professionals. Should you go for creating your own password hashing, some of the things you'd need to take care of include:

- Ensuring pre-image resistance to prevent calculating the input based on the hash output.
- Ensuring high collision resistance to prevent finding two inputs that hash to the same output.
- Randomization and the avalanche effect to make sure attackers can't easily find hashing patterns and correlations between the input and the output.
- Resilience to a wide array of side-channel attacks (that is, attacks based on algorithm implementation details and examining the physical effects caused by invoking the implementation), such as timing attacks and cache attacks.
- Minimizing any efficiency gains attainable by attackers through the use of cracking-optimized hardware such as ASIC, FPGA, and GPUs.

This is a lot on your plate – even more so given that you won't have access to qualified testers from the cryptography community to help you find (inevitable) vulnerabilities.

You'll likely want to depend on secrecy and obscurity by keeping your algorithm private. Doing so breaks the fundamental doctrine of cryptography known as the **Kerckhoff's principle:** "a cryptosystem should be secure even if everything about the system, except the key, is public knowledge." Security by obscurity can provide a short-term advantage but relying on it long-term is a bad practice:

- Hiding vulnerabilities prevents revealing and repairing them as part of an open discussion and increases the probability of exploits.
- If your password database ever leaks, there's a good chance that the source code of your application will leak along with it, and as soon as your untested algorithm becomes known to the attacker, they'll have an easy time cracking it.

You'll put sensitive user data at risk. Leaking sensitive user data is one of the worst things that can happen to a business. This is something that instantly undermines trust, turns customers away, and is very expensive to remediate. Some companies and lots of developers are prone to the Not Invented Here fallacy, but password hashing is probably the worst thing you can choose to re-implement.

Most importantly, you won't know when your algorithm gets broken.

Established algorithms and implementations benefit from years of testing and polishing by large communities of cryptography experts who help reveal and fix vulnerabilities without any malicious intent.

Since your own algorithm and/or implementation won't be available to anyone with a good will, attackers will be the only category of people willing to crack it. Once they do that, they won't give you a heads-up; you'll only know when sensitive data of your users is compromised, and your business is in serious trouble.

But what if you really want to level up your cryptography and learn by doing?

That's great! Go forward and practice. Read reference implementations of existing algorithms, play with your own implementations, reach out to the community for advice, and have a great time learning something new and exciting!

Just don't use whatever you've written in your production applications.

30 'Encryption central to trust, confidentiality, and India's efforts of digital transformation'

by Shruti Dhapola

https://indianexpress.com/article/technology/tech-news-technology/end-to-end-encryption-whatsapp-india-intermediary-rules-interview-internet-society-7100543/lite/#csi=1&referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s

'Breaking encryption is like trying to solve one problem by creating 1000 more.' Noelle de Guzman, Senior Policy Advisor in Asia-Pacific for US-based NGO Internet Society, is unambiguous on encryption and traceability in the Indian context. While India has proposed changes to the 'Intermediary Guidelines' in 2018, which add a traceability clause for messages, cyber-security experts are still skeptical about the changes, which are yet to be finalised.

The Internet Society's new paper on 'Traceability and Cybersecurity' tries to answer whether it is possible to ensure 'traceability' without compromising user privacy and examines some of the possible methods, especially in relation to apps like WhatsApp. The Ministry of Electronics and Information Technology's (MeITY) proposed a change to 'Intermediary Rules' is expected to impact apps like WhatsApp, Signal, Telegram and Wire that thrive on their end-to-end encryption capabilities.

In an email interview with indianexpress.com, Noelle de Guzman explained the challenges and risks around breaking this end-to-end encryption. Edited excerpts from the interaction.

Is traceability actually possible despite end-to-end encrypted apps like WhatsApp without compromising user protection?

Experts had significant concerns around the two technical methods often proposed to enable traceability: the use of digital signatures and the use of metadata. These methods were cited as threats to the privacy and security of users, and their ability to achieve traceability is not clear.

Instead, platforms could be forced to use methods to allow third parties to access the content of communications to comply with traceability requirements – drastically weakening the security and privacy of end-to-end encrypted communications which are fundamental to the protection of Internet users.

What are the risks associated with digital signature methods?

Digital signatures are vulnerable to impersonation, so there is concern that innocent users may be implicated in illegal conduct by cyber criminals that impersonate digital signatures. Experts doubted that digital signatures could be reliably used to attribute a message to its true originator – and achieve traceability.

Digital signatures are also a valuable target for criminals. If the digital signature system was compromised, criminals would have the potential to see when a particular user is sending a message – by receiving and decrypting the originator information. You could envision a scenario where criminals implicate public figures in the sending of illegal content and tailor their impersonation based on the victim's use pattern of the service.

What are the shortfalls of sharing metadata to enforce traceability?

Digital attribution (or traceability) is not absolute, particularly through metadata, making criminal liability hard to establish. It is difficult to tie a user to a message, and criminals could use spoofed metadata to implicate innocent users when sending illegal content. This makes the use of metadata for traceability less useful.

Metadata retained to try to enable traceability is also a valuable target for bad actors. Criminals and foreign adversaries could use the stored metadata to develop social graphs of users or gather information that could enable attacks such as extortion, social engineering, or blackmail. Social graphs could also expose sensitive details of government and elected officials, journalists, activists, lawyers, and dissidents.

What are the major risks when it comes to breaking end-to-end encryption?

Breaking encryption is like trying to solve one problem by creating 1,000 more. The primary risk in breaking end-to-end encryption to access unencrypted data of anyone user is that it puts everyone on that service at risk. If the access method is abused by an employee, leaked, or discovered by bad actors, it can be used to access the data of everyone, undermining security for all. That's why end-to-end encryption is so critical – according to technical experts there is no known way to provide targeted access without undermining security for all.

Authorities also argue that end-to-end encryption is interfering with their investigations. Is there any alternative for them to get the information without breaking encryption? Is that technically possible?

Law enforcement agencies around the world have found creative alternatives to get the information they need without needing to break end-to-end encryption. One method is using classic police work, like turning a key informant. In the investigation into the Mexican drug cartel boss El Chapo, law enforcement convinced the cartel's IT director to help them gain access to the cartel's encrypted communications. Through the informant's cooperation, investigators received access to hundreds of encrypted calls among the crime syndicate.

Another is exploiting existing security vulnerabilities, or government hacking, to get access to encrypted communications. This can be very effective, like in the Encrochat case in Europe, where law enforcement was able to hack an encrypted phone network and make over 800 arrests related to organised crime. However, government hacking is still dangerous, as vulnerabilities could go unpatched and hacking tools can be stolen or escape into the wild. For example, the Petya/NotPetya ransomware was based on Eternal Blue, a US government hacking tool that became public.

Government hacking could have unintended consequences, undermining the confidentiality of the information being transmitted, and the trust that users have in the digital tools and services that they use. Encryption is central to trust and confidentiality, and for India, its efforts to transform into a digitally powered nation and society.

The Indian government should take a multi-stakeholder and whole-of-government approach to the issues at hand, to have a better understanding of what's at stake relative to the threats that they think these proposals will help solve, and to come up with ways to effectively address the root causes behind these issues (misinformation, for instance, can be successfully countered with education, as in the Finland example).

Recently in India, private WhatsApp messages were leaked . . .

This definitely made headlines, but was not the result of an inherent weakness in WhatsApp or tools that can extract data from that service. Users have the option to store their message history on their local device or on cloud services in unencrypted form, where it is vulnerable to hacking just like any other data. To avoid this risk, users can choose not to store their message history, or store it in encrypted form, where even if it is breached it will be unintelligible. Also, as with any service, it is important for users to guard their credentials closely, since if someone gets the user's credentials, they can access the user's data directly.

Third-party access is often given to enable traceability. What are the repercussions of this?

Just as in breaking end-to-end encryption, the repercussions of access for traceability are the risks associated with exposing everyone on the service. Regardless of the technical method used, and the procedural controls surrounding its use, if that method is abused, leaked, or discovered, it can be used by bad actors to trace the communications of all users on that service, undermining the security for everyone.

Current mechanisms to intercept or monitor communications in India lack transparency and sufficient oversight when used (and their effectiveness has been poorly evaluated) – this is not a good precursor for expanding those powers to encrypted services that hundreds of millions of Indian citizens now rely on.

Isn’t client-side scanning a safe means of ensuring traceability?

While client-side scanning – which creates a “hash” of unencrypted content and compares it to known objectionable material – seems like a reasonable approach, it too has risks. In most cases, the hashes are sent to a central database for comparison. This is subject to hacking, where a bad actor could modify the database (for example by adding digital fingerprints) to flag material outside the scope of the government’s stated interest. This would allow them to track to whom, when, and where certain content was communicated. These fingerprints could include commonly used passwords or other information to enable attacks such as social engineering, extortion, or blackmail.

Additionally, in some client-side scanning proposals, an unencrypted version of flagged material is sent for human examination, increasing the risk of abuse or misinterpretation.

Whoever controls or has access to the database (which may include the platform/service provider itself) can also use it to screen for and gather any content of interest, such as information for advertising. Bad actors, including hostile governments, could block users from sending specific content, preventing legitimate content from being shared, and potentially impeding the communications of law enforcement, emergency response, and national security personnel.

Finally, client-side scanning is not a “silver bullet” – sophisticated criminals can manipulate content to change the digital fingerprint and avoid detection, while others can just switch to other services that don’t use client-side scanning to avoid getting caught.

09 Dec 2020

31 Fast quantum random number generator could advance cryptography on the cheap

by Karmela Padavic-Callaghan

https://physicsworld.com/a/fast-quantum-random-number-generator-could-advance-cryptography-on-the-cheap/

While world events are often difficult to predict, true randomness is surprisingly hard to find. In recent years, physicists have turned to quantum mechanics for a solution, using the inherently unpredictable behavior of photons to generate the truly random numbers that underpin many modern cryptographic protocols. Now, a new study promises to make this process of quantum random number generation more accessible, by showing that it is possible to produce certifiably random numbers quickly using a system built with off-the-shelf components.

When numbers are used to securely encode information, the randomness of those numbers is crucial: a string of truly random numbers is one that a hacker can never guess. In classical physics, however, all processes – even chaotic ones – are deterministic, making true randomness impossible. To illustrate this, study lead author David Drahi, a physicist at the University of Oxford, UK, notes that classically, a simple coin flip is about as random as it gets. However, he continues, “if you know the mass of the coin, if you can see the coin, if you can look at the wind, you can predict where it is going to land”. Classical randomness is therefore limited by the existence of information about the physical process meant to produce it.

In the quantum world, in contrast, “there are these fundamentally non-deterministic processes,” says Nathan Walk, a physicist at Freie Universitat Berlin, Germany and a co-author on the study. The results of quantum measurements, he adds, are inherently unpredictable, because their outcome does not exist in any meaningful way until the measurement has been made and the wavefunction of the system has, famously, collapsed.

Certifiably random

In developing their random number generator (RNG), the study's authors focused not only on producing randomness, but also on confirming that this randomness originates from a non-deterministic quantum process rather than some incidental classical noise in the experiment. "There is not a test you can do on a string of numbers to tell if it's random," Walk notes. "You can't certify strings. But you can certify processes."

Drahi, Walk and collaborators built such a quantum certification process – essentially an additional measurement – into their protocol for generating random numbers. They also developed rigorous theoretical proofs of its effectiveness and demonstrated that it can be implemented in practice by performing experiments using quantum light. According to Renato Renner, a physicist at ETH Zurich in Switzerland who was not affiliated with the study, such steps are important for creating a practical system. "You really want to have a device that produces some certificate, otherwise you don't really profit from any quantum advantages," he says.

In their experiments, the researchers send laser light (a photonic state) into one input of a beam splitter while the other input is kept void, resulting in a zero signal (a vacuum state). The consequent pair of output beams is then measured using two separate detectors. Because each photon that arrives at the beam splitter has an equal (50%) chance of being reflected or transmitted, the difference between the numbers of photons recorded by each detector is unpredictable. It is bound to be a random number, Drahi explains.

To confirm that randomness generated in this way is reliable and useful, the researchers performed another measurement on the photonic state before it reaches the beam splitter. In this certification measurement, the light signal is discarded if it would not generate the desired amount of randomness at the end of the experiment. This can happen if the laser signal contains either too few photons or too many. Too few, and the number of possible unpredictable events will be too low for the measurement to be sufficiently random. Too many, and the detectors will hit their maximum value, making the measurement fully predictable.

The inclusion of this certification measurement means that the researchers have theorized and built a device that not only produces randomness at a fast rate of 8.05 gigabits per second, but also ensures the quality of that randomness in real time. According to Feihu Xu, a physicist at the University of Science and Technology of China who was not involved in the work, this "development of a formal framework to monitor and certify the randomness" stands out even though some other ideas in the study have been explored before.

"Untrusted" light source

The researchers' inclusion of real-time randomness certification in their experiment also has consequences for its possible future applications, because the study's theoretical framework proves that the RNG protocol is partly independent of the devices used to implement it. For instance, the light source used can be "untrusted" – the randomness analysis is independent of any information about it. As long as the light signal passes the certification measurement, the properties of the device that produced it do not affect the quality of final randomness. This flexibility means that the group's quantum RNG could in principle be used by "a person or a computer that knows nothing about quantum physics", Walk notes. The numbers obtained in this fashion would be reliably random regardless of operator's expertise, he adds, since the protocol automatically ensures its own performance.

As a bonus, the research team managed to construct their experiment using affordable off-the-shelf components – a feature that allowed Drahi to ship the experimental setup from Oxford to some of his co-authors in Moscow. "It got there and it worked," he says, noting that it would have been virtually impossible to ship all of the components for a more exotic quantum device across a continent, have a different researcher assemble them upon arrival, and then successfully generate random numbers at the same high speed. This level of practicality, combined with the rigorous approach to confirming the randomness of their random numbers as well as generating them, sets up this study as a promising starting point for the development of real-world quantum devices providing reliably true randomness. "It could have very broad applications," Renner concludes.

32 Major breakthrough: Copenhagen researchers can now achieve 'quantum advantage'

by Peter Lodahl & Ravitej Uppu

https://news.ku.dk/all_news/2020/12/major-breakthrough-copenhagen-researchers-can-now-achieve-quantum-advantage/

First came Google. Now, researchers at the University of Copenhagen's Niels Bohr Institute in collaboration with University of Bochum have joined Google in the race to build the world's first quantum computer with what they are calling a "major breakthrough".

"We now possess the tool that makes it possible to build a quantum simulator that can outperform a classical computer. This is a major breakthrough and the first step into uncharted territory in the world of quantum physics," asserts Professor Peter Lodahl, Director of the Center for Hybrid Quantum Networks (Hy-Q).

Specifically, the researchers developed a nanochip less than one-tenth the thickness of a human hair. The chip allows them to produce enough stable light particles, known as photons, encoded with quantum information to scale up the technology, and in so doing, may achieve what is known as 'quantum advantage': the state where a quantum device can solve a given computational task faster than the world's most powerful supercomputer.

A 10 million Euro experiment

While the researchers have yet to conduct an actual 'quantum advantage' experiment, their article in Science Advances proves that their chip produces a quantum mechanical resource that can be used to reach 'quantum advantage' with already demonstrated technology.

To achieve this state demands that one can control about 50 quantum bits, "qubits" – quantum physics' equivalent of the binary bits of zeros and ones used in our classical computers – in a comprehensive experimental set-up that is well beyond the university's own financial means.

"It could cost us 10 million Euro to perform an actual experiment that simultaneously controls 50 photons, as Google did it with superconducting qubits. We simply can't afford that. However, what we as scientific researchers can do is to develop a photon source and prove that it can be used to achieve ‘quantum advantage’. We have developed the fundamental building block,” explains Assistant Professor Ravitej Uppu, lead author of the results.

“In the meantime, we will use our photon sources to develop new and advanced quantum simulators to solve complex biochemical problems that might, for example, be used to develop new medicines. So, we are already preparing the next steps for the technology. Being at a university allows one to establish the foundation of a technology and demonstrate the possibilities, whereas definitive technology upscaling requires greater investment. We will work to establish a strong European consortium of academic and industrial partners with a focus on building photonic quantum simulators with ‘quantum advantage’,” continues Peter Lodahl.

A bright future for upscaling quantum computers

Various schools exist in the world of qubit development for quantum computers, depending upon which “quantum building blocks” one starts with: atoms, electrons, or photons. Each platform has pros and cons, and it remains difficult to predict, which technology will triumph.

The primary advantage of light-based quantum computers is that technology is already available for scaling up to many qubits because of the availability of advanced photonic chips, which have been developed for the telecom industry. A major challenge to generating photon qubits has been to do so with sufficiently high quality. This is precisely where the Copenhagen researchers achieved their breakthrough.

“Denmark and Europe have proud traditions in quantum optics research, and at the same time a strong telecom industry and infrastructure. It would be really exciting to combine these strengths in a large-scale initiative dedicated to photonic quantum computers. It would be fantastic to be part of a process that extends all the way from fundamental quantum physics to new technological applications,” says Peter Lodahl.

Facts:

- Researchers have developed a nanochip capable of producing hundreds of light particles (photons) that can be used to store huge amounts of data in the form of quantum information.
- The nanochip produces light particles containing information, and can be used as hardware in tomorrow’s quantum computers, much in the same way that electrical transistors are used in today’s conventional computers.
- The research is funded by the Danish National Research Foundation, the European Research Council, and the Danish Agency for Science, Technology and Innovation and is a collaboration with the University of Bochum, Germany.

33 IonQ’s roadmap: Quantum machine learning by 2023, broad quantum advantage by 2025

by Emil Protalinski

https://venturebeat-com.cdn.ampproject.org/c/s/venturebeat.com/2020/12/09/ionq-roadmap-quantum-machine-learning-2023-broad-quantum-advantage-2025/amp/

IonQ today laid out its five-year roadmap for trapped ion quantum computers. The company plans to deploy rack-mounted modular quantum computers small enough to be networked together in a datacenter by 2023. That will result in a quantum advantage in building for machine learning, the company expects. IonQ then plans to achieve broad quantum advantage by 2025.

In October, IonQ announced a new 32-qubit quantum computer available in private beta and promised two next-gen computers were in the works. When we asked for a roadmap, the company promised to deliver one "in the next six weeks or so." And here we are.

Quantum computing leverages qubits (unlike bits that can only be in a state of 0 or 1, qubits can also be in a superposition of the two) to perform computations that would be much more difficult, or simply not feasible, for a classical computer. The computational power of a quantum computer can be limited by factors like qubit lifetime, coherence time, gate fidelity, number of qubits, and so on. As a result of all these factors and because the industry is nowhere close to a consensus on what the transistor for qubits should look like, it's difficult to compare quantum computers using a single metric. (It's also difficult to compare classical computers using a single metric, but quantum computing companies are grasping to show their tech is best.)

We talked to IonQ CEO Peter Chapman, who has previously explained how quantum computing will change the future of AI, about how his company put together its roadmap. "Generally our plan over the next couple of years is doubling the number of physical qubits every year to 18 months throughout the decade," Chapman said. "However, physical qubits really don't tell the whole story."

Algorithmic Qubits

IonQ has a new metric, Algorithmic Qubits, that takes the log base 2 of IBM's quantum volume, which also doesn't effectively measure quantum computers. As quantum computers improve, quantum volume quickly becomes unusable because the number grows so quickly. Since its 32-qubit quantum computer achieved a quantum volume of 4 million, IonQ has agreed.

So IonQ defines Algorithmic Qubits as "the largest number of effectively perfect qubits you can deploy for a typical quantum program." The benchmark takes error correction into account, has a direct relationship to qubit count, and represents the number of "useful" encoded qubits in a particular quantum computer. Algorithmic Qubits is a proxy for the ability to execute real quantum algorithms for a given input size.

IonQ has even introduced an Algorithmic Qubit Calculator to help you compare quantum computing systems. Unsurprisingly, IonQ's quantum computers come out on top using this metric.

"Of course, every president in every company says theirs is the best," Chapman said. "You probably take that down for every interview you do for any quantum company. Everyone says theirs is the best and everyone else is junk."

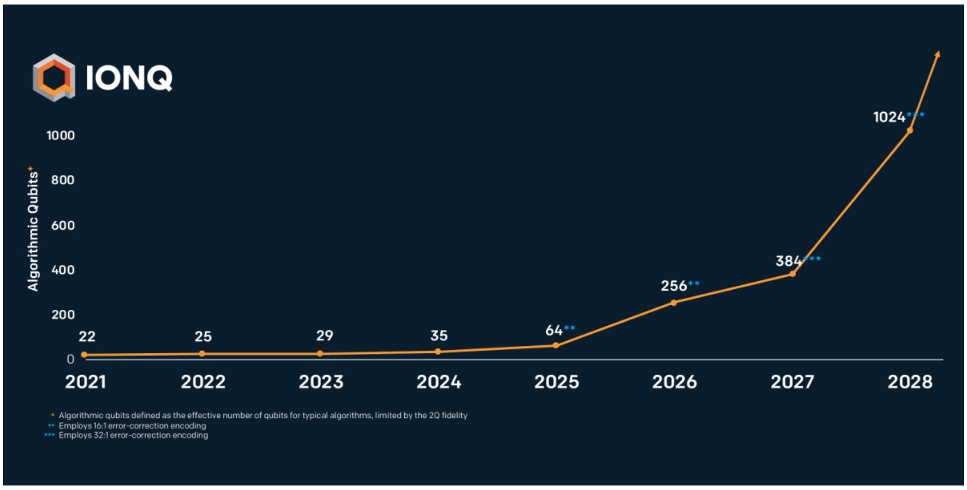
IonQ is hoping Algorithmic Qubits replaces comparisons based on the number of physical qubits. We'll know soon enough whether competitors like IBM, Honeywell, Xanadu, and Psiquantum choose to play ball or not.

Five-year roadmap

Regardless, IonQ is laying out its roadmap using its new Algorithmic Qubits metric. The company will focus on improving the quality of its quantum logic gate operations to continue to increase Algorithmic

Qubits, or usable qubits. It will then work on implementing quantum error correction with low overhead and scaling the number of physical qubits to boost its metric further.

IonQ's recently released 32-qubit system with 99.9% fidelity features 22 Algorithmic Qubits. The chart above shows that its second next-gen quantum computer will feature 29 Algorithm Qubits. "In 2023, we expect to have enough qubits to be able to start early quantum advantage in building for machine learning," Chapman said. "And we've seen in this last year with the 32-qubit system, some early progress that allows these noisy systems to be able to take advantage of machine learning. So I think that will be the lowest-hanging fruit that we can see coming."



* Algorithmic qubits defined as the effective number of qubits for typical algorithms, limited by the 2Q fidelity
** Employs 16:1 error-correction encoding
*** Employs 32:1 error-correction encoding

Broad quantum advantage

IonQ projects that its third next-gen quantum computer coming in 2025 will feature 64 Algorithmic Qubits by employing 16:1 error-correction encoding. In the three years that follow, the Algorithmic Qubits metric will take off further and IonQ will rely on 32:1 error-correction encoding.

"Most people agree at about 72 qubits or so is the place where broad quantum advantage starts," Chapman said. "That's where quantum computers start to take on supercomputers. We're probably looking into a roughly 2024-2025 timeframe for that. How we plan to get there is by 2023 to have a rack-mounted quantum computer, maybe 6U high running at room temperature, and all sitting on a quantum network."

IonQ is using the term "broad quantum advantage" as a measure separate from the quantum supremacy milestones achieved last year by Google and last week by Chinese scientists. "Those things are great science experiments, but they're very academic milestones," Chapman said. "What we're talking about here is a line of application developer sitting at some corporation and making a decision as to whether or not to run it on a quantum computer, on the cloud, or on supercomputers. It's not an academic exercise. It's really at that point where average developers are saying, 'Oh, I think this would be better on a quantum computer.'"

34 Myth vs. reality: a practical perspective on quantum computing

by Julie Love

https://cloudblogs.microsoft.com/quantum/2020/12/09/microsoft-practical-quantum-computing-q2b/

There's a lot of speculation about the potential for quantum computing, but to get a clearer vision of the future impact, we need to disentangle myth from reality. At this week's virtual Q2B conference, we take a pragmatic perspective to cut through the hype and discuss the practicality of quantum computers, how to future-proof quantum software development, and the real value obtained today through quantum-inspired solutions on classical computers.

Achieving practical quantum advantage

Dr. Matthias Troyer, Distinguished Scientist with Microsoft Quantum, explains what will be needed for quantum computing to be better and faster than classical computing in his talk Disentangling Hype from Reality: Achieving Practical Quantum Advantage. People talk about many potential problems they hope quantum computers can help with, including fighting cancer, forecasting the weather, or countering climate change. Having a pragmatic approach to determining real speedups will enable us to focus the work on the areas that will deliver impact.

For example, quantum computers have limited I/O capability and will thus not be good at big data problems. However, the area where quantum does excel is large compute problems on small data. This includes chemistry and materials science, for game-changing solutions like designing better batteries, new catalysts, quantum materials, or countering climate change. But even for compute-intensive problems, we need to take a closer look. Troyer explains that each operation in a quantum algorithm is slower by more than 10 orders of magnitude compared to a classical computer. This means we need a large speedup advantage in the algorithm to overcome the slowdowns intrinsic to the quantum system; we need superquadratic speedups.

Troyer is optimistic about the potential for quantum computing but brings a realistic perspective to what is needed to get to practical quantum advantage: small data/big compute problems, superquadratic speedup, fault-tolerant quantum computers scaling to millions of qubits and beyond, and the tools and systems to develop the algorithms to run the quantum systems.

Future-proofing quantum development

Developers and researchers want to ensure they invest in languages and tools that will adapt to the capabilities of more powerful quantum systems in the future. Microsoft's open-source **Quantum Intermediate Representation (QIR)** and the **Q#** programming language provide developers with a flexible foundation that protects their development investments.

QIR is a new Microsoft-developed intermediate representation for quantum programs that is hardware and language agnostic, so it can be a common interface between many languages and target quantum computation platforms. Based on the popular open-source LLVM intermediate language, QIR is designed to enable the development of a broad and flexible ecosystem of software tools for quantum development.

As quantum computing capabilities evolve, we expect large-scale quantum applications will take full advantage of both classical and quantum computing resources working together. QIR provides full capabilities for describing rich classical computation fully integrated with quantum computation. It's a key layer in achieving a scaled quantum system that can be programmed and controlled for general algorithms.

In his presentation at the Q2B conference, Future-Proofing Your Quantum Development with Q# and QIR, Microsoft Senior Software Engineer Stefan Wernli explains to a technical audience why QIR and Q# are practical investments for long-term quantum development. Learn more about QIR in our recent Quantum Blog post.

Quantum-inspired optimization solutions today

At the same time, there are ways to get practical value today through “quantum-inspired” solutions that apply quantum principles for increased speed and accuracy to algorithms running on classical computers.

We are already seeing how quantum-inspired optimization solutions can solve complex transportation and logistics challenges. An example is Microsoft’s collaboration with Trimble Transportation to optimize its transportation supply chain, presented at the Q2B conference in Freight for the Future: Quantum-Inspired Optimization for Transportation by Anita Ramanan, Microsoft Quantum Software Engineer, and Scott Vanselous, VP Digital Supply Chain Solutions at Trimble.

Trimble’s Vanselous explains how today’s increased dependence on e-commerce and shipping has fundamentally raised expectations across the supply chain. However, there was friction in the supply chain because of siloed data between shippers, carriers, and brokers; limited visibility; and a focus on task optimization vs. system optimization. Trimble and Microsoft are designing quantum-inspired load matching algorithms for a platform that enables all supply chain members to increase efficiency, minimize costs, and take advantage of newly visible opportunities. You can learn more about our collaboration in this video:

Many industries – automotive, aerospace, healthcare, government, finance, manufacturing, and energy – have tough optimization problems where these quantum-inspired solutions can save time and money. And these solutions will only get more valuable when scaled quantum hardware becomes available and provides further acceleration.

How to get started

Explore Microsoft’s quantum-inspired optimization solutions, both pre-built Azure Quantum and custom solutions that run on classical and accelerated compute resources.

Learn how to write quantum code with Q# and the Quantum Development Kit. Write your first quantum program without having to worry about the underlying physics or hardware.

Azure Quantum will be available in preview early next year.

35 Hidden symmetry could be key to more robust quantum systems, researchers find

by University of Cambridge

https://phys.org/news/2020-12-hidden-symmetry-key-robust-quantum.html

Researchers have found a way to protect highly fragile quantum systems from noise, which could aid in the design and development of new quantum devices, such as ultra-powerful quantum computers.

The researchers, from the University of Cambridge, have shown that microscopic particles can remain intrinsically linked, or entangled, over long distances even if there are random disruptions between them. Using the mathematics of quantum theory, they discovered a simple setup where entangled particles can be prepared and stabilized even in the presence of noise by taking advantage of a previously unknown symmetry in quantum systems.

Their results, reported in the journal Physical Review Letters, open a new window into the mysterious quantum world that could revolutionize future technology by preserving quantum effects in noisy environments, which is the single biggest hurdle for developing such technology. Harnessing this capability will be at the heart of ultrafast quantum computers.

Quantum systems are built on the peculiar behavior of particles at the atomic level and could revolutionize the way that complex calculations are performed. While a normal computer bit is an electrical switch that can be set to either one or zero, a quantum bit, or qubit, can be set to one, zero, or both at the same time. Furthermore, when two qubits are entangled, an operation on one immediately affects the other, no matter how far apart they are. This dual state is what gives a quantum computer its power. A computer built with entangled qubits instead of normal bits could perform calculations well beyond the capacities of even the most powerful supercomputers.

“However, qubits are extremely finicky things, and the tiniest bit of noise in their environment can cause their entanglement to break,” said Dr. Shovan Dutta from Cambridge’s Cavendish Laboratory, the paper’s first author. “Until we can find a way to make quantum systems more robust, their real-world applications will be limited.”

Several companies – most notably, IBM and Google – have developed working quantum computers, although so far these have been limited to less than 100 qubits. They require near-total isolation from noise, and even then, have very short lifetimes of a few microseconds. Both companies have plans to develop 1000 qubit quantum computers within the next few years, although unless the stability issues are overcome, quantum computers will not reach practical use.

Now, Dutta and his co-author Professor Nigel Cooper have discovered a robust quantum system where multiple pairs of qubits remain entangled even with a lot of noise.

They modeled an atomic system in a lattice formation, where atoms strongly interact with each other, hopping from one site of the lattice to another. The authors found if noise were added in the middle of the lattice, it didn’t affect entangled particles between left and right sides. This surprising feature results from a special type of symmetry that conserves the number of such entangled pairs.

“We weren’t expecting this stabilized type of entanglement at all,” said Dutta. “We stumbled upon this hidden symmetry, which is very rare in these noisy systems.”

They showed this hidden symmetry protects the entangled pairs and allows their number to be controlled from zero to a large maximum value. Similar conclusions can be applied to a broad class of physical systems and can be realized with already existing ingredients in experimental platforms, paving the way to controllable entanglement in a noisy environment.

“Uncontrolled environmental disturbances are bad for survival of quantum effects like entanglement, but one can learn a lot by deliberately engineering specific types of disturbances and seeing how the particles respond,” said Dutta. “We’ve shown that a simple form of disturbance can actually produce – and preserve – many entangled pairs, which is a great incentive for experimental developments in this field.”

The researchers are hoping to confirm their theoretical findings with experiments within the next year.

36 D-Wave to compare Annealing and Gate-Model Quantum Computers

https://www.swissquantumhub.com/d-wave-to-compare-annealing-and-gate-model-quantum-computers/

D-Wave has just announced a cross-system software tool providing interoperability between quantum annealing and gate-model quantum computers. The open-source plugin allows developers to map quadratic optimization inputs in IBM's Qiskit format onto D-Wave's quadratic unconstrained binary optimization (QUBO) format and solve the same input on any quantum system supported in Qiskit.

The code is available for free as a stand-alone package in GitHub and provides the ability to use, test, solve and compare real applications with both gate-model and annealing quantum computers.

To download and install the cross-paradigm integration plugin for free, click here.

08 Dec 2020

37 Cloudflare and Apple design a new privacy-friendly internet protocol

by Zack Whittaker

https://techcrunch.com/2020/12/08/cloudflare-and-apple-design-a-new-privacy-friendly-internet-protocol/?guccounter=1

Engineers at Cloudflare and Apple say they've developed a new internet protocol that will shore up one of the biggest holes in internet privacy that many don't know even exists. Dubbed Oblivious DNS-over-HTTPS, or ODoH for short, the new protocol makes it far more difficult for internet providers to know which websites you visit.

But first, a little bit about how the internet works.

Every time you go to visit a website, your browser uses a DNS resolver to convert web addresses to machine-readable IP addresses to locate where a web page is located on the internet. But this process is not encrypted, meaning that every time you load a website the DNS query is sent in the clear. That means the DNS resolver – which might be your internet provider unless you've changed it – knows which websites you visit. That's not great for your privacy, especially since your internet provider can also sell your browsing history to advertisers.

Recent developments like DNS-over-HTTPS (or DoH) have added encryption to DNS queries, making it harder for attackers to hijack DNS queries and point victims to malicious websites instead of the real website you wanted to visit. But that still doesn't stop the DNS resolvers from seeing which website you're trying to visit.

Enter ODoH, which builds on previous work by Princeton academics. In simple terms, ODoH decouples DNS queries from the internet user, preventing the DNS resolver from knowing which sites you visit.

Here's how it works: ODoH wraps a layer of encryption around the DNS query and passes it through a proxy server, which acts as a go-between the internet user and the website they want to visit. Because the DNS query is encrypted, the proxy can't see what's inside, but acts as a shield to prevent the DNS resolver from seeing who sent the query to begin with.

"What ODoH is meant to do is separate the information about who is making the query and what the query is," said Nick Sullivan, Cloudflare's head of research.

In other words, ODoH ensures that only the proxy knows the identity of the internet user and that the DNS resolver only knows the website being requested. Sullivan said that page loading times on ODoH are "practically indistinguishable" from DoH and shouldn't cause any significant changes to browsing speed.

A key component of ODoH working properly is ensuring that the proxy and the DNS resolver never "collude," in that the two are never controlled by the same entity, otherwise the "separation of knowledge is broken," Sullivan said. That means having to rely on companies offering to run proxies.

Sullivan said a few partner organizations are already running proxies, allowing for early adopters to begin using the technology through Cloudflare's existing 1.1.1.1 DNS resolver. But most will have to wait until ODoH is baked into browsers and operating systems before it can be used. That could take months or years, depending on how long it takes for ODoH to be certified as a standard by the Internet Engineering Task Force.

38 Error-Prone Quantum Bits Could Correct Themselves, NIST Physicists Show

by Chad Boutin

https://www.nist.gov/news-events/news/2020/12/error-prone-quantum-bits-could-correct-themselves-nist-physicists-show

One of the chief obstacles facing quantum computer designers – correcting the errors that creep into a processor's calculations – could be overcome with a new approach by physicists from the National Institute of Standards and Technology (NIST), the University of Maryland and the California Institute of Technology, who may have found a way to design quantum memory switches that would self-correct.

The team's theory paper, which appears today in the journal Physical Review Letters, suggests an easier path to creating stable quantum bits, or qubits, which ordinarily are subject to environmental disturbances and errors. Finding methods of correcting these errors is a major issue in quantum computer development, but the research team's approach to qubit design could sidestep the problem.

"Error correction complicates an already complicated situation. It usually requires that you build in additional qubits and make additional measurements to find the errors, all of which typically leads to large hardware overhead," said first author Simon Lieu, who works at the Joint Quantum Institute (JQI) and the Joint Center for Quantum Information and Computer Science (QuICS), both collaborations between NIST and the University of Maryland. "Our scheme is passive and autonomous. It does all that extra work automatically."

Designers are experimenting with many approaches to building qubits. One promising architecture is called a photonic cavity resonator. Within its tiny volume, multiple photons can be driven to bounce back and forth between the cavity's reflective walls. The photons, manifesting their wavelike properties in the cavity, combine to form ripple-like interference patterns. The patterns themselves contain the qubit's information. It's a delicate arrangement that, like ripples on a pond's surface, tends to dissipate quickly.

It is also easily perturbed. To work, qubits need peace and quiet. Noise from the surrounding environment – such as heat or magnetic fields emitted by other nearby components – can disturb the interference pattern and ruin the calculation.

Rather than construct an elaborate system to detect, measure and compensate for noise and errors, the team members perceived that if the supply of photons in the cavity is constantly refreshed, the qubit's quantum information can withstand certain amounts and types of noise.

Because the cavity can hold many photons, a qubit involves a substantial number of them, building in some redundancy. In some qubit designs, leaking photons to the environment – a common occurrence – means information gets lost. But rather than defend against this sort of leakage, the team's approach incorporates it. Their cavity's remaining photons would sustain the interference pattern long enough for more photons to enter and replace the missing ones.

A constant stream of fresh photons also would mean that if some photons in the cavity became corrupted by noise, they would be flushed out quickly enough that the damage would not be catastrophic. The interference pattern might waver for a moment, as a pond's ripples would if a small rock fell in with a disturbing splash, but the ripples' pulsating sources would remain consistent, helping the pattern – and its quantum information – to reassert itself quickly.

"It's like adding fresh water," Lieu said. "Any time the information gets contaminated, the fact that you're pushing in water and cleaning out your pipes dynamically keeps it resistant to damage. This overall configuration is what keeps its steady state strong."

The approach would not make the qubits resistant to all types of errors, Lieu said. Some disturbances would still qualify as splashes too dramatic for the system to handle. In addition, the concept applies primarily to the photonic cavities the team considered and would not necessarily help strengthen other leading qubit designs.

The proposed method adds to an arsenal of promising quantum computer error-correction techniques, such as "topological" qubits, which would also be self-correcting but require yet-to-be-made exotic materials. While the team expects the new approach to be particularly useful for quantum computing based on microwave photons in superconducting architectures, it might also find applications in computing based on optical photons.

The team's work builds on previous theoretical and experimental efforts on photonic qubits. Lieu said that other physicists already have laid most of the necessary groundwork to test the team's proposal experimentally.

"We are planning to reach out to experimentalists to test the idea," he said. "They would just need to put a couple of existing ingredients together."

39 Google launches simulator to help researchers develop quantum algorithms

by Aditya Saroha

https://www.thehindu.com/sci-tech/technology/quantum-computer-qubits-google-open-source-qsim-quantum-simulator/article33280550.ece

Google on Monday said it is launching **qsim**, a new open-source quantum simulator to help researchers develop quantum algorithms.

The search-giant has unveiled a new website to get started with qsim and other open-source quantum software.

Researchers can access Google's tools, research initiatives, educational material, latest publications and research repositories from the website.

While students can find educational resources or apply for internships, and developers interested in quantum computing can also join.

Simulators are important tools for writing and debugging quantum code for developing quantum algorithms.

Google said, as currently available quantum processors are prone to noise and don't correct errors, simulators like qsim will allow researchers to explore quantum algorithms under idealized conditions. They also help prepare experiments to run on actual quantum hardware, it added.

According to the Mountain View-based company, qsim can simulate around 30 qubits on a laptop, or up to 40 qubits in Google Cloud.

Google pointed that it uses qsim frequently to test and benchmark quantum algorithms and processors. For instance, it used qsim with Cirq and TensorFlow Quantum, to train quantum Machine learning models involving hundreds of thousands of circuits.

qsim is part of Google's open source ecosystem of software tools that include Cirq, quantum programming framework, ReCirq, a repository of research examples, and TensorFlow Quantum for quantum machine learning.

Researchers who have developed quantum algorithms with Cirq can use qsim by changing one line of code in Colab. Once done, they will experience an instant speedup in their circuit simulations, Google said.

07 Dec 2020

40 Rethinking quantum systems for faster, more efficient computation

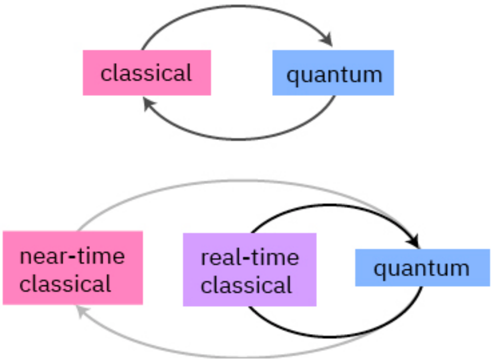
by Ismael Faro, Blake Johnson, and Jay Gambetta

https://www.ibm.com/blogs/research/2020/12/near-real-time-quantum-compute/

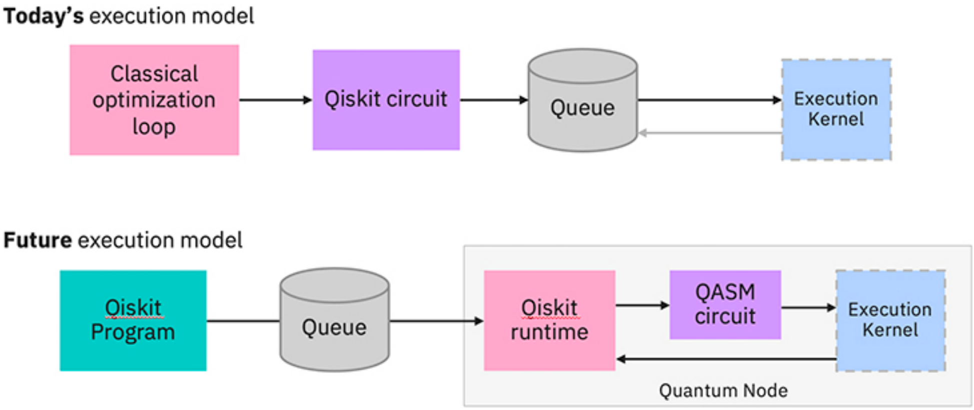
The IBM Quantum team pioneered quantum computing access on the cloud nearly five years ago. Today, members of our community execute billions of circuits each day trying to solve problems in chemistry, optimization, and finance, and have begun developing the first stages of a quantum computing industry. Our team now has defined an aggressive roadmap toward a 1121-qubit machine and beyond – but we need to rethink our software if we hope to maximize the power of what cloud-based quantum computing can do.

Our team is embarking on a journey toward dramatically more efficient execution of quantum workloads. Real workloads require interactions between quantum and classical processors. This is neither surprising nor a novel statement, as even "traditional" quantum algorithms like Shor's algorithm have this structure. However, the advent of near-term applications, such as variational methods, has elevated the importance of efficient execution of jobs with this interactive structure in its inner loop.

As we looked closer at the kinds of jobs our systems execute, we noticed a richer structure of quantum-classical interactions including multiple domains of latency. These domains include real-time computation, where calculations must complete within the coherence time of the qubits, and near-time computation, which tolerates larger latency but which should be more generic. The constraints of these two domains are sufficiently different that they demand distinct solutions.



We're re-thinking the hardware and software architecture of IBM Quantum systems to efficiently handle jobs containing both near-time and real-time elements. For the near-time domain we are exploring concepts for a new runtime that would allow for program execution on classical resources co-located with our quantum hardware. This model removes trips between the user's computer and the quantum hardware for interactive programs, offering significant speed advantages. These programs will be re-usable, allowing people to invoke them many times with different input parameters. We will have more to say about this runtime as we refine our ideas through several iterations of prototypes, but they will define what we are calling a quantum node, which will be the core of future quantum systems showing that a quantum system comprises of quantum processors, software and hardware control stack, and classical computation resources.



For the real-time domain, we are proposing a significant update to the OpenQASM quantum assembly language. This new OpenQASM3 allows for description of a much broader family of circuits containing concurrent classical computation. This is a critical capability to master as we build toward error-mitigated and error-corrected quantum computation. It requires more than just new syntax for circuit construction, though, but also significant changes in the software and hardware control stack that compiles and executes OpenQASM3 circuits. This work is already under way.

Full support of real-time computation in OpenQASM3 will be an extended journey, but you don't have to wait months to begin taking advantage of the first fruits of this labor. In recent weeks we have deployed conditional reset instruction across our fleet of quantum systems. This is a first usable example of simple real-time computation that depends on the low-latency movement of measurement data within our control stack. Already with this feature you can re-use qubits within a circuit, and significantly increase the rate of circuit execution on IBM Quantum hardware.

The net result of the solutions we are developing for near-time and real-time computation will be dramatically more efficient execution of workloads on IBM Quantum systems, allowing us to execute in hours some tasks that previously took days. We hope that these advances will allow us to make quantum computation truly frictionless, where developers can seamlessly take advantage of a quantum systems power without having to worry about the intricacies of the hardware they're programming on. We invite you to join us by running circuits on our quantum systems either by signing up for the open systems here or by joining the IBM Quantum Network to use our advance quantum systems.

06 Dec 2020

41 Quantum Today, Quantum Tomorrow – Some Reflections on 2020 and Views Toward 2021

by K Coleman

https://thequantumdaily.com/2020/12/06/quantum-today-quantum-tomorrow-some-reflections-on-2020-and-views-toward-2021/

As 2020 begins winding down, it is important to examine how far quantum computing and technology (QC&T) has come this year and what is likely to happen in the coming year. This year has certainly been one of advancement. We have seen many new companies created and existing quantum efforts expand.

Perhaps the one term that best describes QC&T in 2020 is unprecedented in the face of a worldwide pandemic and a retreating economy. This continued advancement has caught the attention of many and even some in the education industry worldwide. We have seen a number of organizations in higher education, mostly universities, launch QC&T programs. There have even been a few announcements of efforts to insert quantum related programs in some high schools. It's also wise to recognize the increased growth of published materials (articles, webinars, magazines and white papers) that are now examining practical business uses of quantum computing and technology.

The result of all of this is certainly amplifying the level of awareness and basic understanding of quantum computing and technology and their business applications and implications. So, 2020 has increased the level of interest and QC&T exploration in the general business community and that is a BIG STEP! These actions and so much more combine to make 2020 the year of a leap forward in the advancement and commercialization in the technology lifecycle models of quantum. All of this just scratches the surface of what has taken place in 2020. Now, let's take a glimpse into 2021 and what might await the world in terms of quantum.

It is important to note that no one has the secret formula for accurately predicting the future and that is certainly true in this case. The quantum computing and technology industry movement is likely to see another year of continued growth and formalizations as a new segment of the technology industry. In the United States back in August 2019, the White House announced its plan to increase AI and Quantum Tech funding by 30%. Also, within the U.S. Government, the Department of Energy (DOE) will deploy an exascale computer in 2021 – that is expected to complement DOE's quantum computing initiatives. Also as reported back in 2020, the 1st IBM Quantum Computer will be installed over in Europe early on in 2021.

On top of those events, in 2021, companies will be publicizing specific quantum computing software applications. Many of these are in the latter stages of development already. Perhaps the most important driver of this growth is practical quantum computing and technology use cases that are much more than theory. They are operational in terms of business and creating value. Some of the 2021 operational use cases will likely include artificial intelligence, machine learning, blockchain, robots and advanced IoT sensors. This will result in multiple segments of quantum computing and technology popping up on the radar screens of more executives, boards and business strategist as their anticipated value increases and projected near-term applications become increasingly enticing.

Moving out of basic research into applied research and the very early stages of commercialization will advance in 2021 and have its challenges. I would be remiss if I did not address the current short-fall in educational activities around quantum. The demand for quantum talent will grow once again with a sharp increase in staffing at the Associates, Bachelors, Masters and even professional certification levels. In the coming year, helping to mitigate this short-fall of talent there are a number of quantum related internships that have already been announced and some still have applications being accepted. The contributions an intern could make at this early stage of commercialization should not be underestimated.

As with the advancement of any new or emerging technology, there comes some down-falls/short-falls and the quantum movement will undoubtably experience an increasing number of those starting in the coming year. In 2021, quantum companies will remain challenged and likely the impact will be felt and become much more apparent even hitting the balance sheet. After all, the biggest down-fall/shortfall will be the shortage of quantum computing and technology professionals. You can't grow if you do not have access to qualified talent. There is no quick or easy solution to this issue.

Another concern that is growing is the possibility that in 2021, the quantum computing and technology industry will see the entry of governmental policies and regulations. That impact is a giant unknown as well as what countries will be the first, to author those policies and regulations. We are likely to see a couple of quantum computing and technology initiatives fall short of expectations, fold, or fail to obtain further funding. You can bet those will draw a great deal of media attention as well as from the Doubting-Thomas community. As usual, these will likely get an unfair amount of publicity and in negative commentaries from the naysayers who will be out in force. That will have a noticeable negative effect on many in the QC&T industry.

All that took place in 2020, certainly makes 2021 an exciting year to look forward to. The exact trajectory and velocity of quantum computing and technology point to an industry that will be moving ahead rapidly. And, with all that appears likely to happen in 2021, that year will surpass and expand our vision of the future of this rapidly emerging technology.

05 Dec 2020

42 Keeping secrets in a quantum world and going beyond

by Shubashree Desikan

https://www.thehindu.com/sci-tech/technology/keeping-secrets-in-a-quantum-world-and-going-beyond/article33258829.ece

Every online transaction we make with another person is protected so that a third person cannot read it without the permission of the two people exchanging the information in the first place. This process is called encryption of the data. The first person, say Alice, sends an encrypted message to the second, say Bob. How can Alice ensure that only Bob has the key to the code she has set and a trespasser, say Kate, can see that there is a transaction but cannot intercept it? To use a simple and oft-used analogy – let Alice send a trunk to Bob with a lock on it. Bob receives the trunk and locks it the second time with his own lock, sending it back to Alice. Alice now removes her lock and sends the trunk back to Bob. Bob now can unlock the lock he had put and open the trunk to see the secret message.

Thus, while the transaction took place in full public view, only Alice and Bob were able to read the message inside the trunk.

In the time of the classical computer, the lock in question consists of a problem that is mathematically hard for the computer to solve. For example, Alice takes a two very large prime numbers, that is, numbers that are only divisible by themselves and by one. She multiplies the two and creates an even larger number. She uses this number to encrypt or lock her message to Bob. Kate, now is in trouble because, in order to break the lock, she has to factorise a very large number whose factors are large prime numbers.

This is difficult because if the prime factors are large enough, the problem becomes very difficult to crack for a classical computer. It would take the classical computer "exponentially large" time to guess the factors.

This mathematical problem known as integer factorisation is one of the methods presently used to encrypt our secret or private messages. There are other methods using the so-called discrete logarithm problem, which again would take a normal computer exponentially large time to crack.

Quantum computers

This was all well, as long as we only had to deal with classical computers. Now, enters the quantum computer. One of the basic elements that make up this quantum computer is that where the classical one uses bits to compute this one uses "qubits". What is the difference?

Classical bits can take the value 0 or 1, allowing for a binary system to be set up and the lowest level of computer language is done manipulating these bits. A qubit on the other hand can exist as a superposition of two states 0 and 1. So if you have an n-qubit number, it can exist as a superposition of 2n states. This also allows for immense amount of parallel processing.

Hence the question of whether these problems which are "hard" for the classical computer become easier for a quantum one has the disturbing answer – yes. So, a new cryptography has to be devised, and that is where IIT Madras professor, Shweta Agrawal's work comes into play. She works not just with quantum cryptography but with post quantum cryptography – a field which deals with additional possibilities offered by a quantum system, which goes beyond being able to break the integer factor code.

Enter lattices

One of the main contenders for a mathematical problem that is hard for the quantum computer to crack is the so-called **shortest vector problem**. This involves lattices. Lattices are regular arrangement of points in space; examples in nature include honeycombs and all crystalline solids, like common salt. *A line of regularly spaced points is a lattice in one dimension*, and a crystal of salt is a three-dimensional lattice. Mathematically, we can extend this construction to 5, 10 or even 500 dimensions.

At this magnitude, it becomes in theory a "hard" problem for a quantum computer to calculate the shortest vector from one point to any other point. This problem can therefore be used to construct "locks" that can even withstand a quantum attack. In her work which appeared at conferences Eurocrypt 2019 and

2020, Dr. Agrawal provides new methods to construct such encryption schemes which are secure against quantum computers.

As an example of what one can achieve using such encryption schemes, take two companies which are considering a merger, and want to find out if it will be mutually profitable by engaging in some computation, but without revealing their assets to each other. “We can encrypt the information about their individual assets, and provide a secret key which only reveals the output of the computation and does not reveal anything about the inputs!” says Dr. Agrawal.

Thus, it follows as she says: “In modern cryptography, not only can we create locks on information so that quantum computers cannot break them, we can even design the locks so that the information inside the locks can be manipulated without even opening the locks!”

04 Dec 2020

43 Anne Matsuura: Intel Taking Multi-Pronged Approach at Solving Four Critical Quantum Computing Challenges

by Matt Swayne

https://thequantumdaily.com/2020/12/04/anne-matsuura-intel-taking-multi-pronged-approach-at-solving-four-critical-quantum-computing-challenges/

To get quantum computers out of the lab and into the effort to solve real-world challenges, Intel plans to address each layer of a full quantum stack, according Anne Matsuura, director of Quantum & Molecular Technologies, Intel Labs at Intel Corporation.

Matsuura addressed the crowds gathered virtually at Intel Labs Day 2020 on some of those challenges and some of the opportunities for “**quantum practicality**,” a term Intel uses to describe ways that quantum computers can be used in the real world, such as assisting with drug design and materials research.

“Today’s hundred qubits – or even a thousand qubits – will not get us there, however,” she said. “We will need a full-stack, commercial scale quantum computing system of millions of qubits to attain quantum practicality for this type of ambitious problem-solving.”

The reason that those large numbers of qubits will be needed is due to the exponential computing power – and super sensitivity – of qubits.

“A quantum computer power grows exponentially with the number of qubits,” Matsuura explained. “So, theoretically, if we had 50 of these entangled qubits, we would be able to access more states than any possible super computer, if we had 300 entangled qubits, we could represent more states than atoms in the universe at the same time. It all sounds really powerful, but the qubits are very fragile, they don’t have very long lifetimes. Noise or information causes a loss of information. So, in reality, we’ll need hundreds of thousands – or even more likely – probably millions of high quality qubits for a commercial-sized quantum computer.”

Fortunately, Intel, which has a long history of fitting more and more semiconductors on smaller and smaller chips, knows a thing or two about scaling.

“It is inherent to how we approach technology and innovation – and quantum is no different,” said Matsuura.

To address the challenges of mastering qubit technology, Intel is focusing on spin-qubit technologies, cryogenic control technology and full-stack innovation.

Intel believes that spin-qubit technology lends itself to the scaling challenge compared to other approaches, said Matsuura. It also is an approach that leverages Intel's current manufacturing capabilities, Matsuura said.

She added that this also addresses a key challenge of delivering that quantum practicality – building quality qubits that can be manufactured in large volumes, but ones that also have long lifetimes and produce sufficient connectivity between qubits.

Qubit control is another challenge and it's one that Intel is making progress, according to Matsuura.

In many of today's designs, qubits are controlled by racks of control electronics with complex wiring leading to the qubit, which rest in a cryogenic refrigerator. This would take millions of wires if the design would scale to needed dimensions. Intel's cryogenic qubit control chip technology is developed to maximize qubit control.

Matsuura also said that Intel has a plan to address error correction, another key quantum challenge.

"We are developing noise-resilient quantum algorithms and error mitigation techniques to help us run those algorithms on today's small qubit systems," she said.

The final challenge is building a scalable full stack quantum computer.

"Since quantum computing is an entirely new type of compute, that has an entirely new way of running programs, we need hardware, software and applications developed specifically for quantum," said Matsuura. "This means that quantum computing requires new components at all levels of the stack – from the application, compiler, qubit control processor, control electronics and qubit chip device. Intel is develop all components of the full quantum computing stack."

44 Atos announces Q-score, the only universal metrics to assess quantum performance and superiority

https://www.globenewswire.com/news-release/2020/12/04/2139677/0/en/Atos-announces-Q-score-the-only-universal-metrics-to-assess-quantum-performance-and-superiority.html

Atos introduces "**Q-score**", the first universal quantum metrics, applicable to all programmable quantum processors. Atos' Q-score measures a quantum system's effectiveness at handling real-life problems, those which cannot be solved by traditional computers, rather than simply measuring its theoretical performance. Q-score reaffirms Atos' commitment to deliver early and concrete benefits of quantum computing. Over the past five years, Atos has become a pioneer in quantum applications through its participation in industrial and academic partnerships and funded projects, working hand-in-hand with industrials to develop use-cases which will be able to be accelerated by quantum computing.

"Faced with the emergence of a myriad of processor technologies and programming approaches, organizations looking to invest in quantum computing need a reliable metrics to help them choose the most efficient path for them. Being hardware-agnostic, Q-score is an objective, simple and fair metrics which they can rely on," said Elie Girard, Atos CEO. "Since the launch of 'Atos Quantum' in 2016, the first quantum computing industry program in Europe, our aim has remained the same: advance the development of industry and research applications, and pave the way to quantum superiority."

What does Q-score measure?

Today the number of qubits (quantum units) is the most common figure of merit for assessing the performance of a quantum system. However, qubits are volatile and vastly vary in quality (speed, stability, connectivity, etc.) from one quantum technology to another (such as supraconducting, trapped ions, silicon and photonics), making it an imperfect benchmark tool. By focusing on the ability to solve well-known combinatorial optimization problems, Atos Q-score will provide research centers, universities, businesses and technological leaders with explicit, reliable, objective and comparable results when solving real-world optimization problems.

Q-score measures the actual performance of quantum processors when solving an optimization problem, representative of the near-term quantum computing era (NISQ - Noisy Intermediate Scale Quantum). To provide a frame of reference for comparing performance scores and maintain uniformity, Q-score relies on a standard combinatorial optimization problem, the same for all assessments (the Max-Cut Problem, similar to the well-known TSP – Travelling Salesman Problem). The score is calculated based on the maximum number of variables within such a problem that a quantum technology can optimize (ex: 23 variables = 23 Q-score or Qs).

Atos will organize the publication of a yearly list of the most powerful quantum processors in the world based on Q-score. Due in 2021, the first report will include actual self-assessments provided by manufacturers.

Based on an open access software package, Q-score is built on 3 pillars:

- **Application driven:** Q-score is the only metrics system based on near-term available quantum algorithms and measures a quantum system's capacity to solve practical operational problems;
- **Openness and ease of use:** Universal and free, Q-score benefits from Atos' technology-neutral approach. Its software package, including tools and methodology, does not require heavy computation power to calculate the metrics;
- **Objectiveness and reliability:** Atos combines a hardware-agnostic, technology-agnostic approach with a strong expertise in algorithm design and optimization acquired working with major industry clients and technology leaders in the quantum field. The methodology used to build Q-score will be made public and open to assessment.

A free software kit, which enables Q-score to be run on any processor will be available in Q1 2021. Atos invites all manufacturers to run Q-score on their technology and publish their results.

Thanks to the advanced qubit simulation capabilities of the Atos Quantum Learning Machine (Atos QLM), its powerful quantum simulator, Atos is able to calculate Q-score estimates for various platforms. These estimates take into account the characteristics publicly provided by the manufacturers. Results range around a Q-score of 15 Qs, but progress is rapid, with an estimated average Q-score dating from one year ago in the area of 10 Qs, and an estimated projected average Q-score dating one year from now to be above 20 Qs.

Q-score has been reviewed by the Atos Quantum Advisory Board, a group of international experts, mathematicians and physicists authorities in their fields, which met on December 4, 2020.

Understanding Q-score using the Travelling Salesman Problem (TSP)

Today's most promising application of quantum computing is solving large combinatorial optimization problems. Examples of such problems are the famous TSP problem and the less notorious but as important Max-Cut problem.

Problem statement: a traveller needs to visit N number of cities in a round-tour, where distances between all the cities are known and each city should be visited just once. What is the absolute shortest possible route so that he visits each city exactly once and returns to the origin city?

Simple in appearance, this problem becomes quite complex when it comes to giving a definitive, perfect answer taking into account an increasing number of N variables (cities). Max-Cut is a more generic problem, with a broad range of applications, for instance in the optimization of electronic boards or in the positioning of 5G antennas.

Q-score evaluates the capacity of a quantum processor to solve these combinatorial problems.

Q-score, Quantum Performance, and Quantum Superiority

While the most powerful High Performance Computers (HPC) worldwide to come in the near term (so called "exascale") would reach an equivalent Q-score close to 60, today we estimate, according to public data, that the best Quantum Processing Unit (QPU) yields a Q-score around 15 Qs. With recent progress, we expect quantum performance to reach Q-scores above 20 Qs in the coming year.

Q-score can be measured for QPUs with more than 200 qubits. Therefore, it will remain the perfect metrics reference to identify and measure quantum superiority, defined as the ability of quantum technologies to solve an optimization problem that classical technologies cannot solve at the same point in time.

As per the above, Atos estimates quantum superiority in the context of optimization problems to be reached above 60 Qs.

03 Dec 2020

45 Intel Debuts 2nd-Gen Horse Ridge Cryogenic Quantum Control Chip

https://newsroom.intel.com/news/intel-debuts-2nd-gen-horse-ridge-cryogenic-quantum-control-chip/#gs.mun29t

What's New: At an Intel Labs virtual event today, Intel unveiled **Horse Ridge II**, its second-generation cryogenic control chip, marking another milestone in the company's progress toward overcoming scalability, one of quantum computing's biggest hurdles. Building on innovations in the first-generation Horse Ridge controller introduced in 2019, Horse Ridge II supports enhanced capabilities and higher levels of integration for elegant control of the quantum system. New features include the ability to manipulate and read qubit states and control the potential of several gates required to entangle multiple qubits.

> "With Horse Ridge II, Intel continues to lead innovation in the field of quantum cryogenic controls, drawing from our deep interdisciplinary expertise bench across the Integrated Circuit design, Labs and Technology Development teams. We believe that increasing the number of

> qubits without addressing the resulting wiring complexities is akin to owning a sports car, but constantly being stuck in traffic. Horse Ridge II further streamlines quantum circuit controls, and we expect this progress to deliver increased fidelity and decreased power output, bringing us one step closer toward the development of a ‘traffic-free’ integrated quantum circuit.”
>
> – **Jim Clarke**, Intel director of Quantum Hardware, Components Research Group, Intel

Why It Matters: Today’s early quantum systems use room-temperature electronics with many coaxial cables that are routed to the qubit chip inside a dilution refrigerator. This approach does not scale to a large number of qubits due to form factor, cost, power consumption and thermal load to the fridge. With the original Horse Ridge, Intel took the first step toward addressing this challenge by radically simplifying the need for multiple racks of equipment and thousands of wires running into and out of the refrigerator in order to operate the quantum machine. Intel replaced these bulky instruments with a highly integrated system-on-chip (SoC) that simplifies system design and uses sophisticated signal processing techniques to accelerate setup time, improve qubit performance and enable the engineering team to efficiently scale the quantum system to larger qubit counts.

About the New Features: Horse Ridge II builds on the first-generation SoC’s ability to generate radio frequency pulses to manipulate the state of the qubit, known as qubit drive. It introduces two additional control features, paving the way for further integration of external electronic controls into the SoC operating inside the cryogenic refrigerator.

New features enable:

- **Qubit readout:** The function grants the ability to read the current qubit state. The readout is significant, as it allows for on-chip, low-latency qubit state detection without storing large amounts of data, thus saving memory and power.
- **Multigate pulsing:** The ability to simultaneously control the potential of many qubit gates is fundamental for effective qubit readouts and the entanglement and operation of multiple qubits, paving the path toward a more scalable system.

The addition of a programmable microcontroller operating within the integrated circuit enables Horse Ridge II to deliver higher levels of flexibility and sophisticated controls in how the three control functions are executed. The microcontroller uses digital signal processing techniques to perform additional filtering on pulses, helping to reduce crosstalk between qubits.

Horse Ridge II is implemented using Intel® 22nm low-power FinFET technology (22FFL) and its functionality has been verified at 4 kelvins. Today, a quantum computer operates in the millikelvin range – just a fraction of a degree above absolute zero. But silicon spin qubits – the underpinning of Intel’s quantum efforts – have properties that could allow them to operate at temperatures of 1 kelvin or higher, which would significantly reduce the challenges of refrigerating the quantum system.

Intel’s cryogenic control research focuses on achieving the same operational temperature level for both the controls and silicon spin qubits. Ongoing advances in this area, as demonstrated in Horse Ridge II, represent progress over today’s brute force approaches to scaling quantum interconnects and are a critical element of the company’s longer-term quantum practicality vision.

What’s Next: Intel will present additional technical details from this research during the International Solid-State Circuits Conference (ISSCC) in February 2021.

46 Light-based Quantum Computer Exceeds Fastest Classical Supercomputers

by Daniel Garisto

https://www.scientificamerican.com/article/light-based-quantum-computer-exceeds-fastest-classical-supercomputers/

For the first time, a quantum computer made from photons – particles of light – has outperformed even the fastest classical supercomputers.

Physicists led by Chao-Yang Lu and Jian-Wei Pan of the University of Science and Technology of China (USTC) in Shanghai performed a technique called **Gaussian boson sampling** with their quantum computer, named **Jiŭzhāng**. The result, reported in the journal Science, was 76 detected photons – far above and beyond the previous record of five detected photons and the capabilities of classical supercomputers.

Unlike a traditional computer built from silicon processors, Jiŭzhāng is an elaborate tabletop set-up of lasers, mirrors, prisms and photon detectors. It is not a universal computer that could one day send e-mails or store files, but it does demonstrate the potential of quantum computing.

Last year, Google captured headlines when its quantum computer Sycamore took roughly three minutes to do what would take a supercomputer three days (or 10,000 years, depending on your estimation method). In their paper, the USTC team estimates that it would take the Sunway TaihuLight, the third most powerful supercomputer in the world, a staggering 2.5 billion years to perform the same calculation as Jiŭzhāng.

This is only the second demonstration of quantum primacy, which is a term that describes the point at which a quantum computer exponentially outspeeds any classical one, effectively doing what would otherwise essentially be computationally impossible. It is not just proof of principle; there are also some hints that Gaussian boson sampling could have practical applications, such as solving specialized problems in quantum chemistry and math. More broadly, the ability to control photons as qubits is a prerequisite for any large-scale quantum internet.

"It was not obvious that this was going to happen," says Scott Aaronson, a theoretical computer scientist now at the University of Texas at Austin who along with then-student Alex Arkhipov first outlined the basics of boson sampling in 2011. Boson sampling experiments were, for many years, stuck at around three to five detected photons, which is "a hell of a long way" from quantum primacy, according to Aaronson. "Scaling it up is hard," he says. "Hats off to them."

Over the past few years, quantum computing has risen from an obscurity to a multibillion dollar enterprise recognized for its potential impact on national security, the global economy and the foundations of physics and computer science. In 2019, the the U.S. National Quantum Initiative Act was signed into law to invest more than $1.2 billion in quantum technology over the next 10 years. The field has also garnered a fair amount of hype, with unrealistic timelines and bombastic claims about quantum computers making classical computers entirely obsolete.

This latest demonstration of quantum computing's potential from the USTC group is critical because it differs dramatically from Google's approach. Sycamore uses superconducting loops of metal to form qubits; in Jiŭzhāng, the photons themselves are the qubits. Independent corroboration that quantum computing principles can lead to primacy even on totally different hardware "gives us confidence that in the long term, eventually, useful quantum simulators and a fault-tolerant quantum computer will become feasible," Lu says.

A LIGHT SAMPLING

Why do quantum computers have enormous potential? Consider the famous double-slit experiment, in which a photon is fired at a barrier with two slits, A and B. The photon does not go through A, or through B. Instead, the double-slit experiment shows that the photon exists in a "superposition," or combination of possibilities, of having gone through both A and B. In theory, exploiting quantum properties like superposition allows quantum computers to achieve exponential speedups over their classical counterparts when applied to certain specific problems.

Physicists in the early 2000s were interested in exploiting the quantum properties of photons to make a quantum computer, in part because photons can act as qubits at room temperatures, so there is no need for the costly task of cooling one's system to a few kelvins (about -455 degrees Fahrenheit) as with other quantum computing schemes. But it quickly became apparent that building a universal photonic quantum computer was infeasible. To even build a working quantum computer would require millions of lasers and other optical devices. As a result, quantum primacy with photons seemed out of reach.

Then, in 2011, Aaronson and Arkhipov introduced the concept of boson sampling, showing how it could be done with a limited quantum computer made from just a few lasers, mirrors, prisms and photon detectors. Suddenly, there was a path for photonic quantum computers to show that they could be faster than classical computers.

The setup for boson sampling is analogous to the toy called a bean machine, which is just a peg-studded board covered with a sheet of clear glass. Balls are dropped into the rows of pegs from the top. On their way down, they bounce off of the pegs and each other until they land in slots at the bottom. Simulating the distribution of balls in slots is relatively easy on a classical computer.

Instead of balls, boson sampling uses photons, and it replaces pegs with mirrors and prisms. Photons from the lasers bounce off of mirrors and through prisms until they land in a "slot" to be detected. Unlike the classical balls, the photon's quantum properties lead to an exponentially increasing number of possible distributions.

The problem boson sampling solves is essentially "What is the distribution of photons?" Boson sampling is a quantum computer that solves itself by being the distribution of photons. Meanwhile, a classical computer has to figure out the distribution of photons by computing what's called the "permanent" of a matrix. For an input of two photons, this is just a short calculation with a two-by-two array. But as the number of photonic inputs and detectors goes up, the size of the array grows, exponentially increasing the problem's computational difficulty.

Last year the USTC group demonstrated boson sampling with 14 detected photons – hard for a laptop to compute, but easy for a supercomputer. To scale up to quantum primacy, they used a slightly different protocol, Gaussian boson sampling.

According to Christine Silberhorn, an quantum optics expert at the University of Paderborn in Germany and one of the co-developers of Gaussian boson sampling, the technique was designed to avoid the unreliable single photons used in Aaronson and Arkhipov's "vanilla" boson sampling.

"I really wanted to make it practical," she says "It's a scheme which is specific to what you can do experimentally."

Even so, she acknowledges that the USTC setup is dauntingly complicated. Jiǔzhāng begins with a laser that is split so it strikes 25 crystals made of potassium titanyl phosphate. After each crystal is hit, it reliably spits out two photons in opposite directions. The photons are then sent through 100 inputs, where they race through a track made of 300 prisms and 75 mirrors. Finally, the photons land in 100 slots where they are detected. Averaging over 200 seconds of runs, the USTC group detected about 43 photons per run. But in one run, they observed 76 photons – more than enough to justify their quantum primacy claim.

It is difficult to estimate just how much time would be needed for a supercomputer to solve a distribution with 76 detected photons – in large part because it is not exactly feasible to spend 2.5 billion years running a supercomputer to directly check it. Instead, the researchers extrapolate from the time it takes to classically calculate for smaller numbers of detected photons. At best, solving for 50 photons, the researchers claim, would take a supercomputer two days, which is far slower than the 200-second run time of Jiǔzhāng.

Boson sampling schemes have languished at low numbers of photons for years because they are incredibly difficult to scale up. To preserve the sensitive quantum arrangement, the photons must remain indistinguishable. Imagine a horse race where the horses all have to be released from the starting gate at exactly the same time and finish at the same time as well. Photons, unfortunately, are a lot more unreliable than horses.

As photons in Jiǔzhāng travel a 22-meter path, their positions can differ by no more than 25 nanometers. That is the equivalent of 100 horses going 100 kilometers and crossing the finish line with no more than a hair's width between them, Lu says.

QUANTUM QUESTING

The USTC quantum computer takes its name, Jiǔzhāng, from **Jiǔzhāng Suànshù**, or "The Nine Chapters on the Mathematical Art," an ancient Chinese text with an impact comparable to Euclid's Elements.

Quantum computing, too, has many twists and turns ahead. Outspeeding classical computers is not a one-and-done deal, according to Lu, but will instead be a continuing competition to see if classical algorithms and computers can catch up, or if quantum computers will maintain the primacy they have seized.

Things are unlikely to be static. At the end of October, researchers at the Canadian quantum computing start-up Xanadu found an algorithm that quadratically cut the classical simulation time for some boson sampling experiments. In other words, if 50 detected photons sufficed for quantum primacy before, you would now need 100.

For theoretical computer scientists like Aaronson, the result is exciting because it helps give further evidence against the extended Church-Turing thesis, which holds that any physical system can be efficiently simulated on a classical computer.

"At the very broadest level, if we thought of the universe as a computer, then what kind of computer is it?" Aaronson says. "Is it a classical computer? Or is it a quantum computer?"

So far, the universe, like the computers we are attempting to make, seems to be stubbornly quantum.

02 Dec 2020

47 Open source software security vulnerabilities exist for over four years before detection

by Charlie Osborne

https://www.zdnet.com/article/open-source-software-security-vulnerabilities-exist-for-over-four-years-before-detection-study/

It can take an average of over four years for vulnerabilities in open source software to be spotted, an area in the security community that needs to be addressed, researchers say.

According to GitHub's annual State of the Octoverse report, published on Wednesday, reliance on open source projects, components, and libraries is more common than ever.

Over the course of 2020, GitHub tallied over 56 million developers on the platform, with over 60 million new repositories being created – and over 1.9 billion contributions added – over the course of the year.

"You would be hard-pressed to find a scenario where your data does not pass through at least one open source component," GitHub says. "Many of the services and technology we all rely on, from banking to healthcare, also rely on open source software. The artifacts of open source code serve as critical infrastructure for much of the global economy, making the security of open source software mission-critical to the world."

GitHub launched a deep-dive into the state of open source security, comparing information gathered from the organization's dependency security features and the six package ecosystems supported on the platform across October 1, 2019, to September 30, 2020, and October 1, 2018, to September 30, 2019.

Only active repositories have been included, not including forks or 'spam' projects. The package ecosystems analyzed are Composer, Maven, npm, NuGet, PyPi, and RubyGems.

In comparison to 2019, GitHub found that 94% of projects now rely on open source components, with close to 700 dependencies on average. Most frequently, open source dependencies are found in JavaScript – 94% – as well as Ruby and .NET, at 90%, respectively.

On average, vulnerabilities can go undetected for over four years in open source projects before disclosure. A fix is then usually available in just over a month, which GitHub says "indicates clear opportunities to improve vulnerability detection."

However, the majority of bugs in open source software are not malicious. Instead, 83% of the CVE alerts issued by GitHub have been caused by mistakes and human error – although threat actors can still take advantage of them for malicious purposes.

In total, 17% of vulnerabilities are considered malicious – such as backdoor variants – but these triggered only 0.2% of alerts, as they are most often found in abandoned or rarely-used packages.

According to GitHub, 59% of active repositories on the platform will receive a security alert in the coming year. Over 2020, Ruby and JavaScript have been the most likely to receive an alert.

Defining the 'worst' open source vulnerabilities of 2020 is not an easy task as it depends on the reach of impact – on users and repositories – exploitability, and other factors. Some bugs may immediately come to mind, including Zerologon (CVE-2020-1472) and SMBGhost (CVE-2020-0796), but when it comes to project maintainers, GitHub has named a prototype Pollution in lodash as a top vulnerability.

Tracked as CVE-2020-8203 and issued a severity score of 7.4, the RCE security flaw alone has been responsible for over five million GitHub Dependabot alerts due to lodash being one of the most widely-used and popular npm packages.

The open source community now plays a key role in the development of software, but as with any other industry, vulnerabilities are going to exist. GitHub says that project developers, maintainers, and users should check their dependencies for vulnerabilities on a regular basis and should consider implementing automated alerts to remedy security issues in a more efficient and rapid way.

“Open source is critical infrastructure, and we should all contribute to the security of open source software,” the organization added. “Using automated alerting and patching tools to secure software quickly means attack surfaces are evolving, making it harder for attackers to exploit.”

48 Why Intel believes confidential computing will boost AI and machine learning

by Chris O’Brien

https://venturebeat.com/2020/12/02/why-intel-believes-confidential-computing-will-boost-ai-and-machine-learning/

Companies are collecting increasing amounts of data, a trend that is driving the development of better analytical tools and tougher security. Analysis and security are now converging as confidential computing prepares to deliver a critical boost to artificial intelligence.

Intel has been investing heavily in confidential computing as a way to expand the amount and types of data companies will manage through cloud services. According to Intel Fellow Ron Perez, who works on security architecture with the Intel Data Center Group, the company believes the emerging security standard will allow enterprises and large organizations to explore new ways to share the data needed to fuel AI and machine learning.

“We see this as a long-term effort,” Perez said. “But the reason why we’re investing is that it has the potential to be a huge shift for cloud and utility computing.”

Confidential computing is a standard that moves past policy-based privacy and security to implement safeguards on a deeper technical level. By using encryption that can only be unlocked via keys the client holds, confidential computing ensures companies hosting data and applications in the cloud have no way to access underlying data, whether it is stored in a database or passes through an application.

The concept is gaining momentum because it allows data to remain encrypted even as it’s being processed and used in applications. Because the company hosting the data can’t access it, this security standard should prevent hackers from grabbing unencrypted data when it moves to the application layer. It would also theoretically allow companies to share data, even between competitors, to perform security checks on customers and weed out fraud.

In August 2019, Intel became one of the founding members of the Confidential Computing Consortium, an open source effort managed by the Linux Foundation that aims to develop the hardware and software standards needed to further adoption. Companies like IBM, Google, and Microsoft have begun to highlight their work in this area as a way to encourage large enterprises, particularly in areas such as finance and health care, to put more of their sensitive data in the cloud.

Data security’s future

Perez leads a group of senior technologists at Intel focused on security architecture through a program dubbed Pathfinding. Perez describes it as the “pursuit of interesting challenges that our customers are facing.” In Perez’s case, the goal is to develop a pipeline of security technologies for Intel’s datacenter customers.

Intel began its work in this area before the term “confidential computing” came into vogue, with Perez pointing to the company’s launch of software guard extensions in 2015. The SGXs are security coding built directly into Intel processors that create separate memory enclaves where data could be placed to limit access. This idea of using hardware and software to protect data while allowing it to be processed is at the heart of confidential computing.

Microsoft used these Intel processors for its Azure cloud to enable its own confidential computing service. Last month, Intel announced it was expanding these capabilities in a new generation of its Xeon Scalable platform.

“Our approach has been to drive continuous innovation and deep collaboration with our technology partners to improve the confidentiality and integrity of all data, wherever it is,” Perez said.

Confidential computing and AI

Proponents of confidential computing argue that it will lead to a new wave of cloud innovation as companies become more comfortable putting their most sensitive data online. Perez said that helps drive AI and machine learning in a couple of ways.

The first is indirect. AI and ML have advanced in recent years, thanks to the growing datasets available to refine algorithms. Confidential computing, by bringing even more and richer data online, will benefit that development.

“The main connection to machine learning and artificial intelligence is the fact that we’re generating more and more data,” Perez said. “We’re analyzing this data with various machine learning technologies. And that explosion of data is what’s really driving the interest in confidential computing, whether it’s used for machine learning or not. Machine learning just happens to be one of its main uses.”

No matter the type of underlying data, if it must be decrypted to be used, the security of algorithms it passes through is critical.

“How do you protect these algorithms across this very broad spectrum of use cases?” Perez said. “We see confidential computing as a paradigm shift for cloud computing. The infrastructure providers are providing the capabilities that allow cloud companies to deliver these services as a utility, and they don’t have to take responsibility for the protection of the data themselves.”

Beyond that, confidential computing is enabling different types of collaboration around data to drive machine learning. Perez pointed to the example of a brain tumor project at the University of Pennsylvania.

Penn’s Perelman School of Medicine has teamed up with 29 other health care and research institutions around the world, including in the U.K., Germany, and India. The group is using Intel’s confidential computing to develop a distributed approach to machine learning that allows them to share patient data, including medical imaging. Because such data can remain encrypted while it is being used for machine learning, the group can safely share that data and collaborate in a way that otherwise might not be possible.

That’s critical because data is urgently needed to train machine learning, but no single institution has enough to achieve this on its own. Previously, Penn Medicine and Intel Labs published a study showing that federated learning (a collaborative approach) could train a machine learning model far more effectively than working alone. In this case, the group believes the combination of confidential computing and federated learning will allow them to make rapid breakthroughs in AI models that identify brain tumors.

Merchants are also tapping the ability to allow new types of collaboration for customer and partner data, as are enterprises. While analysts like Gartner believe the real impact of confidential computing may still be several years away, Perez said it is already helping some sectors accelerate their AI and machine learning capabilities in the short term.

“There are multiple aspects of the computing stack that need to be protected,” Perez said. “Confidential computing solves problems that couldn’t be solved before. The concept that I can use any computing capability that may reside in any country around the world and still have some preservation of the privacy and confidentiality of my data, that’s pretty powerful.”

49 Quantum computing could reach the market by 2023, says IBM CEO

by DAVID Z. MORRIS

https://fortune.com/2020/12/01/quantum-computing-could-reach-the-market-by-2023-says-ibm-ceo/

Quantum computing remains a science-fiction catchphrase for many. But according to IBM CEO Arvind Krishna, his company’s clients could be using the technology, and reaping huge benefits, as soon as 2023.

“The impact [of quantum computing] on our clients . . . is going to be in the hundreds of billions of dollars,” Krishna said at today’s Fortune Brainstorm Tech virtual conference. Those benefits will be particularly pronounced in medicine.

“If you want to understand penicillin or caffeine, you can’t do that on a conventional supercomputer, no matter how big you make it,” Krishna explained. The subatomic randomness that gives those precious substances their powerful effects are difficult to model with conventional computers, which consist of simple on-off switches known as bits.

By contrast, a quantum computer can mirror randomness. That’s useful not just for medicine, but materials science, weather forecasting, financial modeling, and other problems that involve huge amounts of data and chaotic interactions.

Quantum computing may eventually help IBM solve a more mundane problem: how to keep revenues growing.

Krishna, who succeeded Ginni Rometty as IBM’s CEO in February of 2020, has long focused on cloud computing services, culminating in the acquisition of Red Hat, which he spearheaded before being named CEO. In October, IBM announced plans to spin out slower-growing parts of its business and to focus on cloud and artificial intelligence. Quantum computing, though less strategically central, would also remain under the IBM umbrella.

Speaking to Fortune’s Aaron Pressman, Krishna focused on IBM’s “hybrid cloud” strategy, which the company says represents a $1 trillion market. IBM’s main goal is not to build their own cloud services, but to help big business manage multiple clouds. That’s an appealing proposition not just because different cloud providers offer different strengths, but because dependence on any one vendor is risky.

In October, IBM reported that its cloud services revenue for the prior 12 months had grown by 25% from the previous 12 months. Krishna said those results are being obscured by slower-growing IBM units, such as IT infrastructure services, and that the planned spinoff will clarify IBM's core strength. The COVID-19 pandemic has dramatically accelerated growth in cloud computing.

The pandemic has also changed how offices work, and Krishna provided some insight into IBM's mindset. Only 10% to 15% of IBM employees, he noted, are working in offices, with the rest still remote. Krishna thinks that shift is basically here to stay.

"We're going to end up with a hybrid model," the CEO said. "[Employees] are going to come into the office for meetings, for serendipity. But I think that 40-hour weeks in the office will be a thing of the past" for most workers.

"The office becomes a place to meet," said Krishna, "Not a cubicle where you do routine work."

50 Amazon is laying the groundwork for its own quantum computer

https://www.livemint.com/technology/tech-news/amazon-is-laying-the-groundwork-for-its-own-quantum-computer-11606898739562.html

Amazon.com Inc. is laying the groundwork for a quantum computer, deepening efforts to harness technology that can crunch in seconds vast amounts of data that take even the most powerful supercomputers hours or days to process.

Amazon has been hiring for a Quantum Hardware Team within its Amazon Web Services Center for Quantum Computing, according to internal job postings and information on LinkedIn. Marc Runyan, a former engineer with NASA's Jet Propulsion Laboratory, lists his title on the professional social network as senior quantum research scientist at Amazon and describes his role as "helping to design and build a quantum computer for Amazon Web Services."

A spokesman for Amazon Web Services, the company's cloud-computing group, declined to comment. Runyan didn't immediately respond to a LinkedIn message.

Proponents of quantum computing say the technology will exponentially improve the processing speed and power of computers, enabling them to simulate large systems and drive advances in physics, chemistry and other fields. Rather than storing information in binary 0s or 1s like classical computers, quantum computers rely on "qubits", which can be both 0 and 1 simultaneously, dramatically increasing the amount of information that can be encoded.

The technology is in its infancy and largely limited to prototypes and demonstrations. Scientists say practical, widespread applications for quantum computers are likely years away.

Among Amazon's recent hires are research scientists focusing on designing a new superconducting quantum device as well as device fabrication. Developing its own quantum computer would let Amazon more closely mirror the approach taken by its major cloud rivals. International Business Machines Corp. first made a quantum computer available to the public in 2016 and has rolled out regular upgrades.

Last year, Alphabet Inc.'s Google said it had built a computer that's reached "quantum supremacy," performing a computation in 200 seconds that would take the fastest supercomputers about 10,000 years. But with the rivalrous spirit that has characterized the race to build a quantum computer, IBM cast doubt on Google's claim. In a blog post, it said that a simulation of Google's task could be done in 2.5 days on a conventional computer with enough hard drive storage, not 10,000 years.

Amazon announced its entry into the arena last year and, in August, launched its first quantum computing service, called Braket, which helps cloud clients experiment with quantum algorithms run on AWS. Once they've designed their algorithms, clients can choose to run them on quantum processing systems built by other companies, including D-Wave Systems Inc., IonQ Inc., and Rigetti Computing. At the time, Amazon noted its interest in developing hardware, but stopped short of announcing plans to build its own computer.

One person briefed on Amazon's plans, but not authorized to discuss them, says the company is using a superconductor model, a similar approach to that used by Google and IBM, among others. The person said Amazon has been on a hiring spree to staff its quantum computing group.

Last year Amazon announced the launch of the AWS Center for Quantum Computing, which aimed to bring together researchers from Amazon, the California Institute of Technology and other academic research institutions to develop new quantum computing technologies.

51 IBM Cloud delivers Quantum-Safe Cryptography

https://www.swissquantumhub.com/ibm-cloud-delivers-quantum-safe-cryptography/

IBM today announced a series of cloud services and technologies designed to help clients maintain the highest available level of cryptographic key encryption protection to help protect existing data in the Cloud and prepare for future threats that could evolve with advances in quantum computing.

The company is now offering quantum-safe cryptography support for key management and application transactions in IBM Cloud®, making it the industry's most holistic quantum-safe cryptography approach to securing data available today.

The new capabilities include:

- **Quantum Safe Cryptography Support:** Through the use of open standards and open source technology, this service enhances the standards used to transmit data between enterprise and Cloud, helping to secure data by using a quantum-safe algorithm.
- **Extended IBM Cloud Hyper Protect Crypto Services:** New capabilities are available to enhance privacy of data in cloud applications, where data sent over the network to cloud applications and sensitive data elements like credit card numbers, are stored in a database that can be encrypted at application-level – supported by the industry's highest level of cryptographic key encryption protection with '**Keep Your Own Key**' (KYOK) capability.

IBM Key Protect, a Cloud-based service that provides lifecycle management for encryption keys that are used in IBM Cloud services or client-built applications, has now introduced the ability to use a quantum-safe cryptography enabled Transport Layer Security (TLS) connection – helping to protect data during the key lifecycle management.

In addition, IBM Cloud is also introducing quantum-safe cryptography support capabilities to enable application transactions. When cloud native containerized applications run on Red Hat® OpenShift® on IBM Cloud or IBM Cloud Kubernetes Services, secured TLS connections can help application transactions with quantum-safe cryptography support during data-in-transit and protect from potential breaches.

Today, IBM Cloud is also delivering new capabilities to help secure application transactions and sensitive data using IBM Cloud Hyper Protect Crypto Services, which offer the industry's highest level of cryptographic key encryption protection by providing customers with 'Keep Your Own Key' (KYOK) capability. Built on FIPS-140-2 Level 4-certified hardware – the highest level of security offered by any cloud provider in the industry for cryptographic modules – this allows clients to have exclusive key control, and therefore authority over the data and workloads protected by the keys.

Designed for application transactions where there is a deeper need for more advanced cryptography, IBM Cloud clients can keep their private keys secured within the cloud hardware security module while offloading TLS to IBM Cloud Hyper Protect Crypto Services to help establish a secure connection to the web server. They can also achieve application-level encryption of sensitive data, such as a credit card number, before it gets stored in a database system. (IBM)

52 Riverlane announces first version of its quantum operating system, Deltaflow.OS

https://www.swissquantumhub.com/riverlane-announces-first-version-of-its-quantum-operating-system-deltaflow-os/

The UK startup Riverlane has just announced that the initial version of its quantum operating system Deltaflow.OS, called '**Deltaflow-on-ARTIQ**', is freely available to the public.

This quantum operating system is both hardware and platform agnostic.

In May 2020, Riverlane revealed that they will lead a consortium which has been awarded a £7.6m grant to build a radically new operating system for quantum computers. In September, they run the first successful trials of Deltaflow.OS, using quantum hardware belonging to trapped-ion company, Oxford Ionics.

The product has been built to enable quantum hardware companies as well as algorithm and app developers to accelerate their research by making collaboration easier and reduce down-time in labs. This version uses simulated hardware and ARTIQ as a backend. ARTIQ is a control system which is widely used in the trapped-ion community. Deltaflow-on-ARTIQ consists of the Deltaflow language (Deltalanguage), and various hardware models on which the language can be run, including an emulator of the ARTIQ control system. The Deltalanguage lets users define a graph of different hardware nodes corresponding to the type of hardware elements found in labs. After defining a programme, users can test it on increasingly realistic hardware models.

53 The Future Is Now: Spreading the Word About Post-Quantum Cryptography

by Dustin Moody

https://www.nist.gov/blogs/taking-measure/future-now-spreading-word-about-post-quantum-cryptography

I consider myself a quiet guy – on a Friday night you can usually find me at home doing crossword puzzles. Public speaking doesn't come naturally to me, and I've never really liked it. Like many people, I get really nervous. So, how did I find myself standing at a podium in front of hundreds of people in Fukuoka, Japan?

I had never traveled that far away from home before. I was also pretty jet-lagged, as I had flown to Fukuoka the day prior. But there I was, giving the opening talk at PQCrypto 2016, the latest in a series of conferences in post-quantum cryptography (PQC). To add to my anxiety, I thought most of the audience knew more about PQC than I did.

Despite these circumstances, I managed to do what I was there to do: announce that the National Institute of Standards and Technology (NIST) was kicking off an international competition to find new quantum-resistant cryptographic systems. The attendees reacted very favorably, knowing this would boost their research in the coming years. As it did, and the NIST PQC competition grew, it took me along for the ride.

Let me back up and explain a little bit.

I came to NIST in 2010 as a postdoc with a one-year-old Ph.D. in mathematics. My dissertation involved something called elliptic curves, which turn out to have some very useful applications in the cryptosystems we use to secure our communications on the internet and elsewhere. In particular, elliptic curve cryptosystems have very short keys and signatures, which take up less memory in comparison to other cryptosystems. It was fascinating to me that such a purely mathematical concept had such an important application in the real world.

NIST publishes cryptography standards so that government agencies know how to safely use crypto. These standards are documents that specify exactly how to implement various cryptographic algorithms in a standard way, so that a user's computer will be able to securely communicate with the intended recipient's computer. NIST's crypto standards are well regarded and are used by most public and private organizations around the world.

It was these kinds of applications that led me to NIST. I spent my first few years here continuing my mathematical research and working on a few projects related to crypto standards. In 2012, my manager Lily Chen asked me to become involved with a new project dealing with post-quantum cryptography. One of the project leaders was moving, and I was asked to take his place. I accepted, even though I knew almost nothing about what PQC was.

The goal of the project was to find cryptosystems which would be safe to use, even in the advent of quantum computers. What's a quantum computer? Good question. A really detailed answer wouldn't fit in this blog post. Informally, quantum computers are machines that would harness the properties of quantum physics to solve certain real-world problems that are beyond the power of our present machines. A lot of very intelligent people have been working on building one, with companies like Google, IBM, Intel, Honeywell and Microsoft all racing to be the first to actually construct a quantum computer large enough to tackle some of these problems. While a quantum computer would lead to some amazing scientific breakthroughs, there would also be a pretty catastrophic impact on some of the cryptosystems we rely on today. In particular, quantum computers would break a few of NIST's standardized crypto algorithms, potentially exposing the sensitive information of anybody using those algorithms. Thus, we were tasked to find new ones to replace them.

As a young professional, I didn't have a lot of experience in managing anything. I was lucky that we had a great team of researchers assembled, all of whom were much smarter than I was. Initially, we mostly read the latest papers in the field, talked to experts and started to do some of our own research. In 2015, we organized a workshop and shortly thereafter published a short report (NISTIR 8105) outlining NIST's view of PQC. All this built momentum, and it was at this point we decided to start taking more concrete action toward standardization.

We decided that we would do a PQC competition like what NIST has done in the past for two of our crypto standards (AES and SHA-3). These competitions are major undertakings and have been quite successful at galvanizing the crypto community to focus evaluation and analysis on selected algorithms. The perfect way to announce this was the upcoming PQCrypto workshop in Japan, where the majority of the researchers in the field would be attending. That's how I ended up there.

We are now several years into the competition and hope to select the new quantum-safe algorithms that NIST will standardize in another year or two. I've learned a lot in this time. I've learned the technical details and the science that underlies PQC, of course. But, I've also grown a great deal professionally. I've organized conferences, managed a diverse team of dedicated experts, written many papers and reports, and interacted with the public as we have steered through the PQC standardization process. There have been many challenges, but so far we feel we have been largely successful at coordinating our efforts with the crypto community, standards organizations and even other nations.

As awareness of the threat that quantum computers pose to cryptography has grown, NIST has been invited to share what it is doing at many venues and with numerous organizations. It's been a unique opportunity to travel to many different countries and speak to a variety of people who want to know how "quantum" will impact them. One of my favorite experiences was speaking to representatives of the auto industry. They are concerned about the impact to security since the crypto that is programmed into cars has to have a long lifespan. I hadn't really known much about the security challenges for cars before.

At some point, I know that the project will slow down, and post-quantum cryptography won't be as high priority as it is right now. Part of me would be just fine with that, so I can go back to a quieter workflow. Yet, I must admit I have enjoyed having some time in the spotlight and the opportunity to develop some new skills and meet new people. I'm grateful that NIST is a place where such exciting (often unexpected) experiences await.

01 Dec 2020

54 Playing pool with $|\psi\rangle$ from bouncing billiard balls to Grover algorithm

https://www.swissquantumhub.com/playing-pool-with%cf%88%e2%9f%a9-from-bouncing-billiard-balls-to-grover-algorithm/

In 2003, with "Playing Pool with π", G. Galperin invented an extraordinary method to learn the digits of π by counting the collisions of billiard balls.

Adam R. Brown at Google has demonstrated an exact isomorphism between Galperin's bouncing billiards and Grover's algorithm for quantum search.

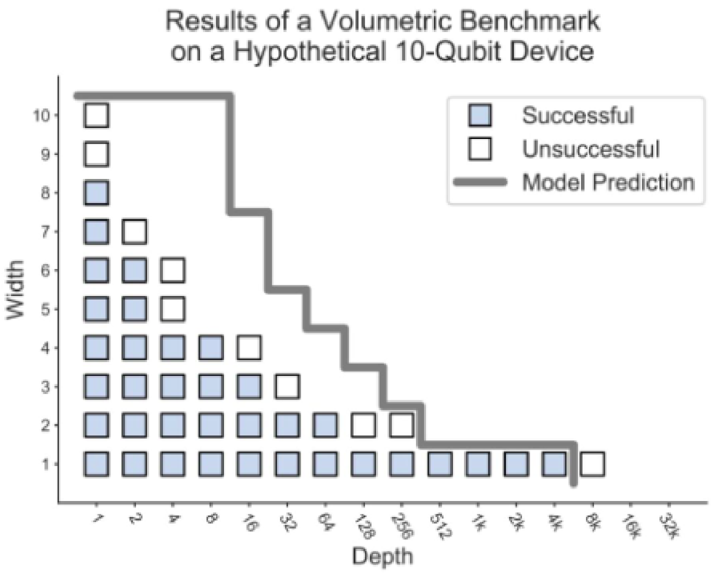
This provides an illuminating way to visualize Grover's algorithm.

55 A volumetric framework for Quantum Computer benchmarks

https://www.swissquantumhub.com/a-volumetric-framework-for-quantum-computer-benchmarks/

Researchers at Sandia National Laboratories propose a very large family of benchmarks for probing the performance of quantum computers.

They call them Volumetric Benchmarks (VBs) because they generalize IBM's benchmark for measuring Quantum Volume.



The **Quantum Volume benchmark** defines a family of square circuits whose depth d and width w are the same. A Volumetric Benchmark defines a family of rectangular quantum circuits, for which d and w are uncoupled to allow the study of time/space performance trade-offs. Each VB defines a mapping from circuit shapes – (w, d) pairs – to test suites $C(w, d)$. A test suite is an ensemble of test circuits that share a common structure. The test suite C for a given circuit shape may be a single circuit C, a specific list of circuits $\{C_1 \ldots C_N\}$ that must all be run, or a large set of possible circuits equipped with a distribution $Pr(C)$.

The circuits in a given VB share a structure, which is limited only by designers' creativity. The team has listed some known benchmarks, and other circuit families, that fit into the VB framework: several families of random circuits, periodic circuits, and algorithm-inspired circuits. The last ingredient defining a benchmark is a success criterion that defines when a processor is judged to have passed a given test circuit.

The scientists have discussed several options. Benchmark data can be analyzed in many ways to extract many properties, but they proposed a simple, universal graphical summary of results that illustrates the Pareto frontier of the d vs w trade-off for the processor being benchmarked.

56 LG Uplus tests commercial usefulness of quantum-resistant cryptography technology

by Lim Chang-won

https://www.ajudaily.com/view/20201201105143491

Quantum-resistant cryptography technology is essential in the era of quantum computing to ensure safe data transmission at hospitals and other places handling sensitive information. It has been applied to corporate lines in a pilot project arranged by LG Uplus, a mobile carrier in South Korea, to verify commercial usefulness.

LG Uplus (LGU+) has partnered with Cheon Jung-hee, a Seoul National University professor of mathematical sciences who heads Cryptolab, a lab involved in encryption and data security, to commercialize post-quantum cryptography (PQC) technology, which refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer.

Even though current, publicly known, experimental quantum computers lack processing power to break any real cryptographic algorithm, many cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat. Quantum computation uses quantum bits or qubits. Theoretically, a quantum computer would gain enormous processing power and perform tasks using all possible permutations simultaneously.

LGU+ said that PQC technology has been applied to 640 kilometers of an exclusive line connecting LG Innotek's plant in Pyeongrtaek and its data center in the southern port city of Busan as well as an exclusive line used by Eulji Medical Center at its buildings in Seoul and Daejeon. LG Innotek is the electric component unit of South Korea's LG Group.

Quantum cryptography is an essential security solution for safeguarding critical information. Data encoded in a quantum state is virtually unhackable without quantum keys which are basically random number tables used to decipher encrypted information. Post-quantum cryptography does not require separate network infrastructure to distribute cryptographic keys because it can be applied flexibly to different sections of wired and wireless networks that require encryption.

LGU+ said PQC technology is useful in hospitals and other areas that handle sensitive information. “PQC is an innovative technology that can provide security services to various terminal areas such as wireless networks, smartphones and Internet of Things as well as wired networks,” Koo Sung-chul, in charge of LGU+'s wired network business, said, adding his company would develop application services specialized for each industry.