Crypto News

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

October 1, 2020

Contents

September 2020

30 Sep 2020

1 New detector breakthrough pushes boundaries of quantum computing

by Aalto University

https://phys.org/news/2020-09-detector-breakthrough-boundaries-quantum.html

Physicists at Aalto University and VTT Technical Research Center of Finland have developed a new detector for measuring energy quanta at unprecedented resolution. This discovery could help bring quantum computing out of the laboratory and into real-world applications. The results have been published today in Nature.

The type of detector the team works on is called a bolometer, which measures the energy of incoming radiation by measuring how much it heats up the detector. Professor Mikko Möttönen's Quantum Computing and Devices group at Aalto has been developing their expertise in bolometers for quantum computing over the past decade, and have now developed a device that can match current state-of-the-art detectors used in quantum computers.

"It is amazing how we have been able to improve the specs of our bolometer year after year, and now we embark on an exciting journey into the world of quantum devices," says Möttönen.

Measuring the energy of qubits is at the heart of how quantum computers operate. Most quantum computers currently measure a qubit's energy state by measuring the voltage induced by the qubit. However, there are three problems with voltage measurements: firstly, measuring the voltage requires extensive amplification circuitry, which may limit the scalability of the quantum computer; secondly, this circuitry consumes a lot of power; and thirdly, the voltage measurements carry quantum noise which introduces errors in the qubit readout. Quantum computer researchers hope that by using bolometers to measure qubit energy, they can overcome all of these complications, and now Professor Möttönen's team have developed one that is fast enough and sensitive enough for the job.

"Bolometers are now entering the field of quantum technology and perhaps their first application could be in reading out the quantum information from qubits. The bolometer speed and accuracy seems now right for it," says Professor Möttönen.

The team had previously produced a bolometer made of a gold-palladium alloy with unparalleled low noise levels in its measurements, but it was still too slow to measure qubits in quantum computers. The breakthrough in this new work was achieved by swapping from making the bolometer out of gold-palladium alloys to making them out of graphene. To do this, they collaborated with Professor Pertti Hakonen's NANO group – also at Aalto University – who have expertise in fabricating graphene-based devices. Graphene has a very low heat capacity, which means that it is possible to detect very small changes in its energy quickly. It is this speed in detecting the energy differences that makes it perfect for a bolometer with applications in measuring qubits and other experimental quantum systems. By swapping to graphene, the researchers have produced a bolometer that can make measurements in well below a microsecond, as fast as the technology currently used to measure qubits.

"Changing to graphene increased the detector speed by 100 times, while the noise level remained the same. After these initial results, there is still a lot of optimisation we can do to make the device even better," says Professor Hakonen.

Now that the new bolometers can compete when it comes to speed, the hope is to utilize the other advantages bolometers have in quantum technology. While the bolometers reported in the current work performs on par with the current state-of-the-art voltage measurements, future bolometers have the potential to outperform them. Current technology is limited by Heisenberg's uncertainty principle: voltage measurements will always have quantum noise, but bolometers do not. This higher theoretical accuracy, combined with the lower energy demands and smaller size – the graphene flake could fit comfortably inside a single bacterium – means that bolometers are an exciting new device concept for quantum computing.

The next steps for their research is to resolve the smallest energy packets ever observed using bolometers in real-time and to use the bolometer to measure the quantum properties of microwave photons, which not only have exciting applications in quantum technologies such as computing and communications, but also in fundamental understanding of quantum physics.

Many of the scientists involved in the researchers also work at IQM, a spin-out of Aalto University developing technology for quantum computers. "IQM is constantly looking for new ways to enhance its quantum-computer technology and this new bolometer certainly fits the bill," explains Dr. Kuan Yen Tan, Co-Founder of IQM who was also involved in the research.

29 Sep 2020

2 ID Quantique and SK Broadband selected to build a pilot QKD infrastructure in public, medical and industrial sectors in Korea

by Catherine Simondi

https://www.idquantique.com/id-quantique-and-sk-broadband-selected-to-build-a-pilot-qkd-infrastructure-in-public-medical-and-industrial-sectors-in-korea/?utm_term=Read%20more&utm_campaign=QuEST%3A%20Quantum%20Era%20Security%20Times%20September%202020&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-QuEST%3A%20Quantum%20Era%20Security%20Times%20September%202020-_-Read%20more

ID Quantique (IDQ), the world leader in Quantum-Safe security solutions and SK Broadband, Korea's telecom media service provider today announced that they have been selected to build a pilot QKD infrastructure, as part of South Korea's ambitious New Deal plan which was unveiled on September 3rd. The plan encompasses 10 major projects mostly in the digital and green sectors.

As part of the "digital new deal" initiative which covers artificial intelligence, 5G mobile connectivity as well as quantum technologies and aims at creating future growth engines for the post-Corona era, security of data for the long term was identified as a key topic. Building a pilot quantum key distribution (QKD) infrastructure in Korea is a priority to enhance security in 16 use cases in the public, medical, and industrial sectors. This move by the Korean government is very important to ensure long-term security of critical infrastructure, which are at risk from quantum computing, a technology rapidly progressing towards practical applications (as illustrated for example by a recent advance by the University of Chicago). The government is planning a W58 trillion (42.5 billion euros) project investment for the digital sectors with an expected 0.9M jobs created by 2025.

The Korean Ministry of Science, ICT and Technology selected three operators: SK Broadband which collaborates with ID Quantique, as well as KT, and LG U+ to initiate the deployment of a QKD infrastructure. SK Broadband will use ID Quantique's leading QKD products to connect 17 sites and ensure ultra-secure communications in 5 uses cases: Gwangju Metropolitan city network for public sector, Yonsei Medical Center network for healthcare sector and Hanwha systems, Wooribank and CJ Olive networks for industrial sector.

At ID Quantique, we are dedicated to the success of our customers in all areas. We focus on providing high-performance quantum-safe security solutions for the protection of data in transit. By upgrading existing network encryption products with Quantum Key Distribution (aka quantum cryptography) IDQ ensures that the solutions are "quantum-safe". Based on the laws of quantum mechanics, QKD enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. Our solutions protect sensitive data into and beyond the quantum era when quantum computers, which are being built now, will render most of today's conventional encryption algorithms vulnerable.

> "It is thrilling to lead the Quantum Key Distribution market and industry. We deploy the world's top class in Quantum Key Distribution technology, with a current commercial security solution while also preparing for future-use next generation systems. SK Broadband is actively contributing to the development of the QKD ecosystem and will continue pioneering migration towards next generation best-in-class telecommunications."
>
> – Park Chan-Woong, Head of Infra Division, SK Broadband

> "Sensitive data is increasingly in danger from the growing threat of cyberattacks and more and more companies and governments are highly concerned by this issue. We are honoured to be part of the "Digital New Deal project" with SK Broadband to build one of the largest quantum communication infrastructure in the world and thus contributing to establishing a highly secure digital economy."
>
> – Grégoire Ribordy, CEO and co-founder of ID Quantique

3 CERN meets quantum technology

by Matthew Chalmers

https://phys.org/news/2020-09-cern-quantum-technology.html

Today's information and communication technology grew out of the invention and development of quantum mechanics during the last century. But, nifty as it is that billions of transistors can be packed into your smartphone or that photons are routed around the internet with the help of lasers, the devices underpinning the "first quantum revolution" merely rely on the weird properties of quantum mechanics – they don't put them to use directly.

The CERN Quantum Technology Initiative (QTI), which was announced by CERN Director-General Fabiola Gianotti in June, sees CERN join a rapidly-growing global effort to bring about a "second quantum revolution" – whereby phenomena such as superposition and entanglement, which enable an object to be in two places at the same time or to influence another instantaneously, are exploited to build new computing, communication, sensing and simulation devices.

It is difficult to predict the impact of such quantum technologies on society, but for high-energy physics and CERN the benefits are clear. They include advanced computing algorithms to cope with future data-analysis challenges, ultrasensitive detectors to search for hidden-sector particles and gravitational waves, and the use of well-controlled quantum systems to simulate or reproduce the behavior of complex many-body quantum phenomena for theoretical research.

Though relatively new to the quantum technologies scene, CERN is in the unique position of having in one place the diverse set of skills and technologies – including software, computing and data science, theory, sensors, cryogenics, electronics and material science – necessary for such a multidisciplinary endeavor. AEgIS at CERN's Antiproton Decelerator, which is able to explore the multi-particle entangled nature of photons from positronium annihilation, is one of several examples of existing CERN experiments already working in relevant technology areas. CERN also provides valuable use cases to help compare classical and quantum approaches to certain applications, as demonstrated recently when a team at Caltech used a quantum computer comprising 1098 superconducting qubits to "rediscover" the Higgs boson from LHC data. CERN's rich network of academic and industry relations working in unique collaborations such as CERN openlab is a further strength.

The path to CERN's QTI began with a workshop on quantum computing in high-energy physics organized by CERN openlab in November 2018, which was followed by several initiatives, pilot projects and events. During the next three years, the initiative will assess the potential impact of quantum technologies on CERN and high-energy physics on the timescale of the HL-LHC (late 2030s) and beyond. Governance and operational instruments are being finalized and concrete R&D objectives are being defined in the four main quantum technologies areas: computing; sensing and metrology; communication; and simulation and information processing. The CERN QTI will also develop an international education and training program in collaboration with experts, universities and industry, and identify mechanisms for knowledge sharing within the CERN Member States, the high-energy physics community, other scientific research communities and society at large.

"By taking part in this rapidly growing field, CERN not only has much to offer, but also stands to benefit directly from it," says Alberto Di Meglio, coordinator of the CERN QTI and head of CERN openlab. "The CERN Quantum Technology Initiative, by helping structure and coordinate activities with our community and the many international public and private initiatives, is a vital step to prepare for this exciting quantum future."

4 Microsoft taps LLVM for quantum computing

by Paul Krill

https://www.infoworld.com/article/3583993/microsoft-taps-llvm-for-quantum-computing.html

Microsoft has introduced an intermediate representation for quantum programs, called **QIR** (Quantum Intermediate Representation), to serve as a common interface between programming languages for gate-based quantum computing and target quantum computation platforms.

Introduced September 23 and based on the LLVM intermediate language, QIR specifies rules to represent quantum constructs in LLVM. No extensions or modifications to LLVM are necessary.

QIR supports Microsoft's open source Q# language for developing quantum algorithms but is not specific to Q#. Any language for gate-based quantum computing can be represented. QIR also is hardwareagnostic, not specifying a quantum instruction or gate set.

One application cited as being enabled by QIR involves using the LLVM-based Clang compiler to compile QIR into executable machine code for a classical target, providing a path to build a simulator in C or C++ by implementing quantum instruction set functions.

Microsoft has made the draft QIR specification available in the new Q# language repository on GitHub. The company has also rolled out a compiler extension that generates QIR from Q#; it can be found in the feature/QIR branch of the Q# compiler repository. Directions for using the extension have been posted, as well.

Microsoft said that as quantum computing capabilities mature, most large-scale quantum applications will take advantage of both classical and quantum resources working together. LLVM offers QIR capabilities for describing rich classical computation integrated with quantum computation. LLVM also supports integration with many classical languages and tools already supported by the LLVM tool chain.

A common pattern in compilers is to start by compiling the source language into an intermediate representation, typically designed to allow different source languages to be represented. With this intermediate representation, code can be optimized and transformed. Once the actual target execution platform is known, the intermediate representation can be compiled to executable code.

Through an intermediate representation, many source languages can share a common set of optimizers and executable generators. Also, it becomes easy to compile a single source language for many different targets. The intermediate representation provides a common platform to be shared across sources and targets and allows re-use in compiler machinery.

Microsoft anticipates more advances in how classical and quantum computations interact at the hardware level. With QIR, the goal is to provide a single representation that can be used for both current restricted capabilities and more powerful systems in the future. The community will be able to develop optimizations and code transformations.

5 MAPPING THE CHALLENGES IN QUANTUM COMPUTING FOR SOFTWARE DEVELOPERS

by Astha Oriel

https://www.analyticsinsight.net/mapping-challenges-quantum-computing-software-developers/

Quantum Computing is in the nascent stage, yet this technology is a game-changer in the technological revolution. With its advanced computing skills, countries and tech organizations compete to take the sword of Quantum Supremacy. As the heavy investments are made in the research and development of this technology, while chalking out various methods to understand the potential of quantum computing, software developers are rendered to face some of the major challenges associated with this technology.

The report by BCC Research states that The global quantum computing market is expected to reach US$1.3 billion by 2027 at a CAGR of 52.9% from 2022 to 2027 and US$161 million by the year 2022, with a CAGR of 37.3% between 2017-2022.

In its fourth annual conference Quantum Challenge, IBM constituted four major exercises that would help the classic software developers, researchers, and even business owners to understand the aspect of quantum programming. In the four day event, 18 IBM Quantum systems on IBM were utilized by more than 1000 participants from 45 different countries to understand the tenants of Quantum Computing.

Abe Afsaw, Global Lead, Quantum Education, and Open Science IBM, in an interview, elucidate the challenges faced by software developers with programming the Quantum Systems and solutions for how to avoid them. In this article, we will observe the key points cited by Abe to counter these challenges.

Building A Quantum Circuit

Unlike the traditional computing systems, which already have an established circuit, Quantum systems require creating a quantum circuit for easy computation. This is the first exercise, which Abe says will help in understanding the protocol of Quantum programming. The Quantum circuit involves putting on quantum gates on different qubits.

Understanding the Terminologies of Quantum Programming

The terminologies of Quantum programming are fairly different from Classical computing. It involves understanding new processes, strictly associated with Quantum programming, with no reference to the traditional computing model. For the traditional software developer, who anticipates learning Quantum programming, understanding these terminologies and processes, without any detailed source of information becomes a challenge. To counter this and help the software developers to gain knowledge about Quantum computing Abe informed that IBM has released an open-source textbook, which involves learning material and exercises for solving the problem.

The three rules of Quantum Algorithms

Unlike classical computing algorithms, quantum programs have three rules for the algorithm that makes them different from traditional computing. Abe describes the first rule to be the presence of **quantum noise** that can alter the desired outcomes. Quantum noise is the disturbance produced while the Quantum circuit is made to run on the Quantum Systems. The classical system measures the communication and produces the desired outcome by measuring the running the same programs repeatedly to take a vote and understand what the user is trying to communicate. This is called as '**Standard Error Mitigation Technique**.'

However, in quantum programming, repeated communication can destroy the information, and can give online one particular outcome instead of the large Superposition of states for accessibility of the Quantum state. That's why Abe emphasizes that the error mitigation techniques of quantum computing are different from that of classical computing and involves rules for formulating Quantum Algorithms.

The two hardest parts while working on quantum programming is that the measurements are different from the real system and that the principles of quantum mechanics are different from that of the traditional computing applications. In Quantum programming, Superposition plays a key role. Abe describes Superposition as the ability of Quantum programming to take a quantum state and have it become a combination of different basis states to have interference between quantum states and to have entanglement between quantum systems.

Leveraging Quantum Key Distribution

For making Quantum Computing effective in everyday life, Abe rules out applying Quantum key distribution so that that different quantum states can be measured, and quantum communication is secure. The earliest protocol for key distribution, as described by Abe is BB84, where B and B stand for Charles Bennett and Bassard, who developed this protocol in 1984.

This protocol involves the sharing of information from point A to B, with eavesdroppers in the middle, who are named as Alice and Bob. The main idea behind this protocol is taking advantage of the quantum mechanics for identifying the interference in the communication network of Quantum programming.

Solving Problems with Various Solutions

A quantum system is heavily governed by Quantum circuits, which involves a series of operations applied to the qubits in the quantum program. Each circuit has a matrix, which corresponds to the series of operations that are applied. But the hardest part, as observed by Abe in such type of approach, is that the matrix is vast, making it challenging to identify the circuit over which the matrix is generated. Hence to rectify this, the small matrix must be utilized by the software developers with an assortment of solutions, with a deep understanding of things.

By formulating different solutions, the chances of learning are very high.

Conclusion

The future of different sectors looks promising with quantum computing, according to Abe. However, as the technology is still evolving, it will take years for its proper utilization in the large stage. For software developers to counter the challenges of Quantum programming, it becomes imperative to understand the tenants and terminologies of Quantum Computing and look for solutions that can be applied in quantum computing.

6 The Inconvenient Truth About Quantum Computing

by Viraj Kulkarni

https://science.thewire.in/the-sciences/quantum-computing-qubits-error-correction-no-cloning-theorem/

We are in the middle of what the journal Nature has called the “quantum gold rush”. Governments around the world are ramping up their investments in quantum computing. Venture capitalists are pouring billions of dollars into startups sprouting out of university departments. Established technology companies like IBM, Google, Microsoft, Intel, Amazon and Honeywell have recruited highly qualified teams to build quantum computers.

On the websites of these companies, you will find a dazzling array of offerings – ranging from software libraries for quantum computing to consulting services. Their slick marketing collaterals may lead you into thinking quantum computers are already commonplace and are routinely being used to solve problems in finance, transportation, materials science, energy and defence, etc.

But if you look beyond the shiny whitepapers and posters, you might be disappointed. For all their promises of the future, humankind still doesn’t have a working quantum computer that can solve problems of practical importance faster than your laptop can. The ones we have are barely more than lab prototypes, and the promises are erected on the speculative profits of billions of dollars in the future. These prospects aren't yet real.

So when will we build a useful quantum computer?

Experts stand divided on this question. Some say it will take five years; many others estimate it will take decades. A vocal minority has argued we won't have one anytime in the foreseeable future.

A classical computer operates with bits that take the value of either 0 or 1. Quantum bits, or qubits, on the other hand can exist simultaneously as both 0 and 1, much like Schröndinger's cat can be both dead and alive. This property of being in two states at the same time is known as superposition. Quantum computers can leverage superposition to execute multiple computational paths simultaneously, giving them their incredible power.

But unlike classical bits, qubits are extremely fragile. The physical objects that represent classical bits are made up of semiconductors. You can drop them on a table and they would still work fine. But if you so much as bumped against a table on which there is a functional qubit, it will break. Qubits are even affected by seemingly insignificant disturbances like stray electromagnetic waves, vibrations, temperature fluctuations and possibly cosmic rays.

Such tremendous physical brittleness is not the effect of the materials a qubit is made of but because the effects of quantum mechanics are inordinately sensitive to external conditions.

Qubit entanglement

Qubits can maintain superposition only for infinitesimally small intervals of time. Even the slightest interaction with the environment causes a qubit to collapse into a discrete state of either 0 or 1. This is called decoherence. And even before they decohere, random noise caused by non-ideal circuit elements can corrupt the state of the qubits, leading to computing errors.

All computational systems, including classical computers, suffer from numerical errors. To handle errors in classical computers, scientists have developed error-correcting algorithms that rely on redundancy. That is, the computer represents each logical bit by multiple physical bits. If a small number of physical bits is corrupted due to noise, say, the remaining bits can still be used to detect and correct the error.

For example, the logical bit 1 is represented by three physical bits, 111. If one of the physical bits gets corrupted to yield 101, we can still infer the correct value of the logical bit to be 1.

The no-cloning theorem in quantum mechanics says that we can't make perfect copies of a qubit's state. This means we can't directly use classical error-correcting algorithms for quantum computers.

To further complicate things, the act of measuring a qubit causes it to 'collapse' from a superposition of states to a single, discrete state. As a result, the error-correcting algorithm needs to detect and correct errors without interacting with the qubits.

Fortunately, although qubits can't be copied, they can be entangled. When we entangle two qubits with each other, their individual quantum states fuse to form a single joint state. In this setup, if we measure one qubit from a pair of entangled qubits, our act of measurement will instantaneously affect the other qubit as well, and its state will change in a predictable way.

So by constructing a grid of entangled physical qubits to represent a single logical qubit, we can detect and correct quantum-computing errors. And the larger the grid, the more errors we can correct.

Quantum computers need sophisticated electronic circuits to initialise qubits before beginning a computation; perform a variety of mathematical operations on them via quantum gates; and measure the results afterwards. These activities need to be performed with high precision at ultra-low temperatures while keeping the qubits strictly isolated from the environment throughout the process. But however hard we try, some unavoidable disturbances inevitably produce small errors.

If the rate of these errors exceeds a certain threshold, entangling multiple qubits only increases the noise in the system instead of reducing it. So for error correction to work, it is vitally important that we become able to control qubits with an error rate that is below this threshold. We have still not been able to do this.

The largest quantum computers we have today consist of fewer than 100 qubits. IBM announced earlier in September that it plans to build a 1,000-qubit quantum computer by 2023.

Computers perform mathematical operations on data. In order to solve a problem, a quantum computer needs enough qubits to represent the input and store the output – in addition to the qubits required to process intermediate results of the computation. Researchers estimate that a quantum computer will need between 1,000 to 100,000 logical qubits to solve computational problems encountered in practice.

And to keep errors in check, we will need to represent each logical qubit by 1,000 to 100,000 physical qubits – depending on how well we can control the qubits. All together, we will need a few million qubits to make quantum computers perform useful work that is also reliable.

From the point of view of quantum physics, a system with a million qubits is an enormously complex thing. Since qubits can exist in superpositions of two values at a time, a system of N qubits can encode 2^N states. A quantum computer with just 300 qubits will thus have more states than the total number of atoms in the entire universe.

Nobody has figured out exactly how we are going to control such large quantum systems while keeping errors in check. Small, focused groups are working on these challenges at universities and technology companies – but the rest of the community has largely ignored them. Computer science researchers are designing algorithms for quantum computers. Software companies are releasing platforms and libraries to implement these algorithms. Many members of both groups seem to have assumed that sufficiently large quantum computers will be available soon.

Quantum winter

By itself, this is not a problem. Many algorithms in computer science were also designed at a time when we didn't have the hardware to run them. In physics, it is common for theoretical results to precede experimental confirmation by decades. Physicists predicted the existence of the Higgs boson in 1964; it was found at the Large Hadron Collider 48 years later.

The problem arises when the hype surrounding a technology fuels a misleading impression that the technology will be available shortly, and with certain abilities. Sensational headlines have been inflating our expectations of quantum computers, especially of their imminence. University students have been organising quantum hackathons. Network security companies are thinking of becoming 'quantum-proof'.

More problematically, investors seeking short-term returns on their investments are pouring millions into machines that don't yet exist. And large companies, out of fear of missing out on the action, are aggressively pitching quantum solutions. Amazon Web Services and Microsoft have respectively launched products called Braket and Azure Quantum, which purportedly allow developers to access quantum computers in the cloud. However, offerings like these are typically rudimentary circuits without any error-correction or classical algorithms that simulate qubits.

This situation is quite similar to the hype surrounding artificial intelligence in the 1960s. Encouraging results in machine translation and game-playing algorithms led researchers to believe that true artificial intelligence was almost ready. The New York Times reported in 1958, “The Navy revealed the embryo of an electronic computer today that it expects will be able to walk, talk, see, write, reproduce itself and be conscious of its existence.”

When the tall promises didn’t materialise, the hype gave way to disappointment. People who had been sold on tall promises became disillusioned. Investors lost faith in AI and funds dried up. A prolonged period of inactivity followed, known today as the ‘AI winter‘. Faster processing speeds and larger datasets eventually fulfilled some of these promises but only in the last decade – almost sixty years after they were first made. Many more promises remain unfulfilled.

As things stand, we are multiple breakthroughs away from building commercially viable quantum computers. Robust qubits that last longer without decohering will reduce the degree of redundancy required. Better control over qubits will allow us to implement more complex circuits. Better error-correction techniques will enable us to correct more errors using fewer qubits.

Scientists will achieve all these breakthroughs someday – but this day lies in our future, not in our past. And to those who don’t acknowledge this reality, a quantum winter is coming.

7 D-Wave releases its next-generation quantum annealing chip

by JOHN TIMMER

https://arstechnica.com/science/2020/09/d-wave-releases-its-next-generation-quantum-annealing-chip/

Today, quantum computing company D-Wave is announcing the availability of its next-generation quantum annealer, a specialized processor that uses quantum effects to solve optimization and minimization problems. The hardware itself isn’t much of a surprise – D-Wave was discussing its details months ago – but D-Wave talked with Ars about the challenges of building a chip with over a million individual quantum devices. And the company is coupling the hardware’s release to the availability of a new software stack that functions a bit like middleware between the quantum hardware and classical computers.

Quantum annealing

Quantum computers being built by companies like Google and IBM are general-purpose, gate-based machines. They can solve any problem and should show a vast acceleration for specific classes of problems – or they will, as soon as the gate count gets high enough. Right now, these quantum computers are limited to a few-dozen gates and have no error correction. Bringing them up to the scale needed presents a series of difficult technical challenges.

D-Wave’s machine is not general-purpose; it’s technically a quantum annealer, not a quantum computer. It performs calculations that find low-energy states for different configurations of the hardware’s quantum devices. As such, it will only work if a computing problem can be translated into an energy-minimization problem in one of the chip’s possible configurations. That’s not as limiting as it might sound, since many forms of optimization can be translated to an energy minimization problem, including things like complicated scheduling issues and protein structures.

It’s easiest to think of these configurations as a landscape with a series of peaks and valleys, with the problem-solving being the equivalent of searching the landscape for the lowest valley. The more quantum devices there are on D-Wave's chip, the more thoroughly it can sample the landscape. So ramping up the qubit count is absolutely critical for a quantum annealer's utility.

This idea matches D-Wave's hardware pretty well, since it's much easier to add qubits to a quantum annealer; the company's current offering has 2,000 of them. There's also a matter of fault tolerance. While errors in a gate-based quantum computer typically result in a useless output, failures on a D-Wave machine usually mean the answer it returns is low-energy, but not the lowest. And for many problems, a reasonably optimized solution can be good enough.

What has been less clear is whether the approach offers clear advantages over algorithms run on classical computers. For gate-based quantum computers, researchers had already worked out the math to show the potential for quantum supremacy. That isn't the case for quantum annealing. Over the last few years, there have been a number of cases where D-Wave's hardware showed a clear advantage over classical computers, only to see a combination of algorithm and hardware improvements on the classical side erase the difference.

Across generations

D-Wave is hoping that the new system, which it is terming Advantage, is able to demonstrate a clear difference in performance. Prior to today, D-Wave offered a 2,000 qubit quantum optimizer. The Advantage system scales that number up to 5,000. Just as critically, those qubits are connected in additional ways. As mentioned above, problems are structured as a specific configuration of connections among the machine's qubits. If a direct connection between any two isn't available, some of the qubits have to be used to make the connection and are thus unavailable for problem solving.

The 2,000 qubit machine had a total of 6,000 possible connections among its qubits, for an average of three for each of them. The new machine ramps up that total to 35,000, an average of seven connections per qubit. Obviously, this enables far more problems to be configured without using any qubits to establish connections. A white paper shared by D-Wave indicates that it works as expected: larger problems fit in to the hardware, and fewer qubits need to be used as bridges to connect other qubits.

Each qubit on the chip is in the form of a loop of superconducting wire called a Josephson junction. But there are a lot more than 5,000 Josephson junctions on the chip. "The lion's share of those are involved in superconducting control circuitry," D-Wave's processor lead, Mark Johnson, told Ars. "They're basically like digital-analog converters with memory that we can use to program a particular problem."

To get the level of control needed, the new chip has over a million Josephson junctions in total. "Let's put that in perspective," Johnson said. "My iPhone has got a processor on it that's got billions of transistors on it. So in that sense, it's not a lot. But if you're familiar with superconducting integrated circuit technology, this is way on the outside of the curve." Connecting everything also required over 100 meters of superconducting wire – all on a chip that's roughly the size of a thumbnail.

While all of this is made using standard fabrication tools on silicon, that's just a convenient substrate – there are no semiconducting devices on the chip. Johnson wasn't able to go into details on the fabrication process, but he was willing to talk about how these chips are made more generally.

This isn't TSMC

One of the big differences between this process and standard chipmaking is volume. Most of D-Wave's chips are housed in its own facility and get accessed by customers over a cloud service; only a handful are purchased and installed elsewhere. That means the company doesn't need to make very many chips.

When asked how many it makes, Johnson laughed and said, “I’m going to end up as the case of this fellow who predicted there would never be more than five computers in this world,” before going on to say, “I think we can satisfy our business goals with on the order of a dozen of these or less.”

If the company was making standard semiconductor devices, that would mean doing one wafer and calling it a day. But D-Wave considers it progress to have reached the point where it’s getting one useful device off every wafer. “We’re constantly pushing way past the comfort zone of what you might have at a TSMC or an Intel, where you’re looking for how many 9s can I get in my yield,” Johnson told Ars. “If we have that high of a yield, we probably haven’t pushed hard enough.”

A lot of that pushing came in the years leading up to this new processor. Johnson told Ars that the higher levels of connectivity required a new process technology. “[It’s] the first time we’ve made a significant change in the technology node in about 10 years,” he told Ars. “Our fab cross-section is much more complicated. It’s got more materials, it’s got more layers, it’s got more types of devices and more steps in it.”

Beyond the complexity of fashioning the device itself, the fact that it operates at temperatures in the milli-Kelvin range adds to the design challenges as well. As Johnson noted, every wire that comes in to the chip from the outside world is a potential conduit for heat that has to be minimized – again, a problem that most chipmakers don’t face.

Making software easier

The new chip is being made available at the same time as a major change is coming to the software that controls it. One way to solve problems is to understand the nature of the problem and the hardware at sufficient detail to know how to set the connections on the chip so that the results it returns answer the problem. But that’s pretty highly specialized knowledge, and it’s outside the sort of expertise most companies have on hand. So D-Wave is attempting to make it easier by providing an intervening software step that gets rid of some of the complexity.

Under the new system, users will have to understand how to convert their problem into something called a “**quadratic unconstrained binary optimization**,” or QUBO. But if they can do that, they can hand the QUBO to something D-Wave is calling its “hybrid problem solver,” which will do everything needed to get it to execute on the quantum annealer.

This is part of a general trend toward what have been termed “hybrid solutions” for quantum computing, a trend that’s taking place on both the gate-based and annealing platforms. Researchers have acknowledged that the parts of an algorithm that actually perform best on quantum systems are often only a part of a larger computer science problem, and the other parts may perform just fine – or even better – on classical computer hardware. So the full solution to a problem will require a mix of classical and quantum calculations. As is the case here, this can involve using the classical side to figure out how best to program the quantum side.

For D-Wave systems, the possibilities are even more complex. As mentioned above, one of the challenges of exploring energy minimization landscapes on a quantum annealer is figuring out how to fit enough of the landscape into a limited number of qubits. And there are a lot of ways to potentially tackle that issue. Some problems can be divided up into smaller chunks that are then run separately. In other cases, it’s possible to examine the QUBO and find ways of optimizing it so that it fits into the available hardware better.

Other solutions involve doing some calculations on each side of the quantum divide. It’s possible to do a sparse sampling of the landscape on classical hardware and then get the quantum annealer to focus on those areas that seem to look promising. Alternately, you could use the quantum annealer to sparsely sample and then use the classical computer to exhaustively explore the areas around any low-energy solutions it returns.

New users can worry about all these potential ways of handling their problems if they want to, but they can now simply turn the issue over to the hybrid solver and let it do the worrying for them instead. And D-Wave is hoping that this will vastly expand its potential user base. “There’s a lot less work to be done if you don’t have to take them all the way down to the machine language and become experts in all the parameter tuning,” D-Wave VP of Software Murray Thom told Ars. “Offsetting that to a hybrid solver means that businesses can focus on formulating their problems, getting their preproduction tests done, and solving them at scale.”

But is it faster?

The obvious question left after all of this is whether the new hardware and software is ultimately faster than a purely classical solution. But that’s a more complicated question than it initially seems. D-Wave is almost certainly going to be able to identify cases where its hardware outperforms classical algorithms as they now stand. But if the past is any guide, that will motivate computer scientists to give those algorithms a careful look – and possibly find ways of optimizing them further. Performance claims are more of a conversation among experts than they are in the supercomputing space, where there are widely accepted benchmarks.

Perhaps more important is the issue of whether any businesses can find specific cases where the quantum annealing delivers them useful solutions faster than existing algorithms. And that may not require D-Wave’s machine to return answers faster in every case than classical algorithms, since businesses may only need to solve problems under a specific set of circumstances. D-Wave’s ability to return solutions that may not be the most optimal could provide an advantage, since “really good” may be just as useful for businesses as “the best.”

D-Wave is pretty confident that this generation, or possibly the next, will be the point where there’s a clear advantage to using its hardware. But evaluating that claim will mean waiting for both users and computer scientists to spend more time on it.

28 Sep 2020

8 Quantum entanglement realized between distant large objects

by Niels Bohr Institute

https://phys.org/news/2020-09-quantum-entanglement-distant-large.html

A team of researchers at the Niels Bohr Institute, University of Copenhagen, have succeeded in entangling two very different quantum objects. The result has several potential applications in ultra-precise sensing and quantum communication and is now published in Nature Physics.

Entanglement is the basis for quantum communication and quantum sensing. It can be understood as a quantum link between two objects which makes them behave as a single quantum object.

Researchers succeeded in making entanglement between a mechanical oscillator – a vibrating dielectric membrane – and a cloud of atoms, each acting as a tiny magnet, or what physicists call “spin.” These very different entities were possible to entangle by connecting them with photons, particles of light. Atoms can be useful in processing quantum information and the membrane – or mechanical quantum systems in general – can be useful for storage of quantum information.

Professor Eugene Polzik, who led the effort, states that: “With this new technique, we are on route to pushing the boundaries of the possibilities of entanglement. The bigger the objects, the further apart they are, the more disparate they are, the more interesting entanglement becomes from both fundamental and applied perspectives. With the new result, entanglement between very different objects has become possible.”

To understand entanglement, sticking to the example of spins entangled with a mechanical membrane, imagine the position of the vibrating membrane and the tilt of the total spin of all atoms, akin to a spinning top. If both objects move randomly, but if observed moving right or left at the same time, that is called a correlation. Such correlated motion is normally limited to the so-called zero-point motion – the residual, uncorrelated motion of all matter that occurs even at absolute zero temperature. This limits knowledge about any of the systems.

In their experiment, Eugene Polzik’s team entangled the systems, which means that they move in a correlated way with a precision better than the zero-point motion. “Quantum mechanics is like a double-edged sword – it gives us wonderful new technologies, but also limits precision of measurements which would seem just easy from a classical point of view,” says a team member, Michał Parniak. Entangled systems can remain perfectly correlated even if they are at a distance from each other – a feature that has puzzled researchers from the very birth of quantum mechanics more than 100 years ago.

Ph.D. student Christoffer Østfeldt explains further: “Imagine the different ways of realizing quantum states as a kind of zoo of different realities or situations with very different qualities and potentials. If, for example, we wish to build a device of some sort, in order to exploit the different qualities they all possess and in which they perform different functions and solve a different task, it will be necessary to invent a language they are all able to speak. The quantum states need to be able to communicate, for us to use the full potential of the device. That’s what this entanglement between two elements in the zoo has shown we are now capable of.”

A specific example of perspectives of entangling different quantum objects is quantum sensing. Different objects possess sensitivity to different external forces. For example, mechanical oscillators are used as accelerometers and force sensors, whereas atomic spins are used in magnetometers. When only one of the two different entangled objects is subject to external perturbation, entanglement allows it to be measured with a sensitivity not limited by the object’s zero-point fluctuations.

There is a fairly immediate possibility for application of the technique in sensing both for tiny oscillators and big ones. One of the biggest scientific pieces of news in recent years was the first detection of gravity waves, made by the Laser Interferometer Gravitational-wave Observatory (LIGO). LIGO senses and measures extremely faint waves caused by astronomical events in deep space, such as black hole mergers or neutron star mergers. The waves can be observed because they shake the mirrors of the interferometer. But even LIGO’s sensitivity is limited by quantum mechanics because the mirrors of the laser interferometer are also shaken by the zero-point fluctuations. Those fluctuations lead to noise preventing observation of the tiny motion of the mirrors caused by gravitational waves.

It is, in principle, possible to generate entanglement of the LIGO mirrors with an atomic cloud and thus cancel the zero-point noise of the mirrors in the same way as it does for the membrane noise in the present experiment. The perfect correlation between the mirrors and the atomic spins due to their entanglement can be used in such sensors to virtually erase uncertainty. It simply requires taking information from one system and applying the knowledge to the other. In such a way, one could learn both about the position and the momentum of LIGO's mirrors at the same time, entering a so-called quantum-mechanics-free subspace and taking a step towards limitless precision of measurements of motion. A model experiment demonstrating this principle is on the way at Eugene Polzik's laboratory.

9 Seeqc Cuts Its Own Path to the Quantum Era With Integrated Circuit Approach

by Matt Swayne

https://thequantumdaily.com/2020/09/28/tqd-exclusive-seeqc-cuts-its-own-path-to-the-quantum-era-with-integrated-circuit-approac/

Surrounded by corporate giants entering the quantum fray, like Google, IBM and Honeywell, Seeqc may look like a quantum David to a half-dozen or so Goliaths, but, rather than slings and stones, the company says it will rely on a unique approach to quantum technology – and a growing number of key partnerships across the quantum ecosystem – to compete in this competitive field of giants.

Based in Elmsford, NY, and with facilities in the UK and EU, the company has a good corporate role model, according to Oleg Mukhanov, who serves as the startup's Co-CEO and CTO, as well as being a company co-founder.

A few months ago, Michael Neilsen, who is an authority on quantum computing and a co-author of a seminal book about it, tweeted that he "expects the Intel (or at least Fairchild) of quantum computing will likely either be founded in the next 5 years, or already exists." "We're hoping that it's us," Mukhanov said.

That Fairchild in question was a pioneering firm in the manufacturing semiconductor transistors combined into integrated circuits starting the revolution in the electronics industry which changed the landscape of computing and a majority of other industries. Mukhanov is hoping that, by integrating classical and quantum superconducting circuits into a single module, Seeqc will inspire that same type of revolution based on their quantum twist of the integrated circuit design.

The company, which was founded in 2019, considers itself the QC industry's first truly integrated quantum-classical computing system. The technology is based on combining highly energy-efficient single-flux quantum (SFQ) classical digital quantum management co-processor with superconducting quantum processor in a single cryogenic module.

Basically, what that means is the company's chipset is a multichip module that combines the quantum and digital superconducting chips. According to the team, the benefit of that is that quantum computers running on this design would be more robust, faster, more easily scalable, and would greatly simplify the system design.

Just as Intel's, Fairchild's – and other companies that followed – integrated chips bridged the world of big classical computers to laptop sized computing devices, Seeqc's technology is designed to bridge the divide between big, expensive and supersensitive quantum computing installations to more practical quantum computers with much wider application space.

This would address some of the disadvantages of conventional quantum approaches, according to Mukhanov which makes them look like a physics experiment rather than a computer. Seeqc design could replace racks of expensive, high energy, analogue microwave circuitry with proprietary digital chips that are co-located with qubit chips as multi-chip modules in the same 'cryocooled' system or cryostat.

Some companies, like Intel, Microsoft and Google, are investigating if cryogenically cooled CMOS circuits can perform these functions inside of the cryostat. This turns out to be quite challenging, since CMOS produces significant heat – it generates a higher level of heat the faster it operates, Mukhanov said. It overloads the cryostat and generates lots of noise degrading quantum computing fidelity.

In contrast, superconducting SFQ circuits can comfortably operate at millikelvin while generating orders of magnitude less heat and working at a much faster rate than CMOS. Moreover, Mukhanov said that SFQ logic is manufactured of the same material as superconducting qubits making their integration natural.

Superconducting ultra-low power and fast clock SFQ digital logic has been developed for multiple applications including classical computing. In these applications, the cryogenic nature of superconductivity was viewed as a liability, so customers would use this technology only when the extreme performance would be required. For everything else, conventional semiconductor CMOS technology was good enough while conveniently operating at room temperatures.

This changed when quantum computing came around. Cryogenically cooled to millikelvin, superconducting qubits need fast and low power logic for control and readout functions, preferably as close to the qubits as possible, according to Mukhanov.

10 Research Team Claims a Major Advance in Error Correction for Quantum Devices

by Matt Swayne

https://thequantumdaily.com/2020/09/28/research-team-claims-a-major-advance-in-error-correction-for-quantum-devices/

A team of researchers say they're a step closer to fault-tolerant quantum devices, a key factor in building practical quantum computers.

In a study, available on Arxiv, the researchers report they experimentally demonstrated fault-tolerant preparation, rotation, error syndrome extraction and measurement on a logical qubit encoded in the 9-qubit Bacon-Shor code. They added that the result is an encoded logical qubit whose logical fidelity exceeds the fidelity of the entangling operations used to create it

In the paper, the researchers said, "These results show that fault-tolerant quantum systems are currently capable of logical primitives with error rates lower than their constituent parts. With the future addition of intermediate measurements, the full power of scalable quantum error-correction can be achieved."

Theoretically, quantum computers could solve problems in speeds that classical computers cannot achieve. The researchers add that some areas that quantum computers could solve models of important physical processes, optimize complex cost functions and challenge cryptographic methods. However, the failure rates on quantum computers are currently too high to to achieve these results in a practical sense.

The team embedded the 9 data qubits and 4 ancilla qubits of the BaconShor-13 code in a single chain of 15 ions.

According to the researchers, future research will look at demonstrating a tranversal CNOT logical gate that outperforms a two-qubit gate.

“This experiment should be possible in the current system given that two-qubit gates on 23 data qubits have recently been demonstrated,” said the researchers. “Additionally, multiple rounds of error-correction can be achieved by breaking the ion chain to perform mid-circuit detection48 . This shuttling will likely require sympathetic cooling schemes, which have been previously demonstrated and can be readily implemented in this system.”

11 UHS hospitals hit by reported country-wide Ryuk ransomware attack

by Sergiu Gatlan

https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/

Universal Health Services (UHS), a Fortune 500 hospital and healthcare services provider, has reportedly shut down systems at healthcare facilities around the US after a cyber-attack that hit its network during early Sunday morning.

UHS operates over 400 healthcare facilities in the US and the UK, has more than 90,000 employees and provides healthcare services to approximately 3.5 million patients each year.

The Fortune 500 corporation had annual revenues of $11.4 billion in 2019 and it is 330th on Forbes’ ranking of US largest public companies.

Attacked during the night

According to reports coming from UHS’ employees, UHS hospitals in the US including those from California, Florida, Texas, Arizona, and Washington D.C. are left without access to computer and phone systems.

At the moment the affected hospitals are redirecting ambulances and relocating patients in need of surgery to other nearby hospitals.

“When the attack happened multiple antivirus programs were disabled by the attack and hard drives just lit up with activity,” one of the reports reads.

“After 1min or so of this the computers logged out and shutdown. When you try to power back on the computers they automatically just shutdown.

“We have no access to anything computer based including old labs, ekg’s, or radiology studies. We have no access to our PACS radiology system.”

Employees were also told to shut down all systems to block the attackers’ from reaching all devices on the network.

Ryuk ransomware behind the attack

While UHS has made no official statement regarding the attack, reports coming from employees show all the signs of a ransomware attack, starting with its launch during the night to avoid detection before encrypting as many systems as possible and the immediate shut down of all systems after it was discovered to prevent more devices getting locked.

An employee told BleepingComputer that, during the cyberattack, files were being renamed to include the **.ryk** extension. This extension is used by the **Ryuk ransomware**.

Another UHS employee told us that one of the impacted computers' screens changed to display a ransom note reading "Shadow of the Universe," a similar phrase to that appearing at the bottom of Ryuk ransom notes.

Based on information shared with BleepingComputer by Advanced Intel's Vitali Kremez, the attack on UHS' system likely started via a phishing attack.

According to Kremez, their Andariel intelligence platform detected both the Emotet and TrickBot Trojans affecting UHS Inc. throughout 2020, and more recently, in September 2020.

The Emotet trojan is spread via phishing emails containing malicious attachments that install the malware on a victim's computer.

After some time, Emotet will also install TrickBot, which ultimately opens a reverse shell to the Ryuk operators after harvesting sensitive information from compromised networks.

Once the Ryuk actors manually get access to the network they start with reconnaissance and, after gaining admin credentials, they deploy ransomware payloads on network devices using PSExec or PowerShell Empire.

Unfortunately, if this is a ransomware attack, there is also a high chance of the attackers stealing patient and employee data which will further increase the damage.

Last week, BleepingComputer reported that a ransomware attack affecting a German hospital led to the death of a patient in a life-threatening condition after it was redirected to a more distant hospital.

Four deaths were also reported after the incident impacting UHS' facilities, caused by the doctors having to wait for lab results to arrive via courier. BleepingComputer has not been able to independently corroborate if the deaths were related to the attack.

BleepingComputer has contacted UHS for more information about the attack but has not heard back.

27 Sep 2020

12 Swiss Trio Promise Sustainable Future With Photonic & Quantum Tech

by James Dargan

https://thequantumdaily.com/2020/09/27/swiss-trio-promise-sustainable-future-with-photonic-quantum-tech/

The École polytechnique fédérale de Lausanne (EPFL) is one of the most respected institutions of higher learning in Switzerland, and specializes in the natural sciences and engineering. Founded as the École spéciale de Lausanne back in 1853, it gained federal status in 1969. With past alumni Daniel Borel (co-founder of Logitech) and 2017 co-winner of the Nobel Prize in Chemistry Jacques Dubochet to boast of, the EPFL has a top-notch reputation in many fields.

So it's good to hear about a quantum computing (QC) spinout from there, Miraex.

Miraex

Founded in 2019, the startup is focussed on photonic and quantum full-stack solutions for next-generation sensing, networking and computing. Miraex joins the likes of ETH Zurich Quantum Engineering Center, ID Quantique, QRL, and Terra Quantum in the Swiss QC arena.

> MIRAEX PROPRIETARY TECHNOLOGY IS AT THE CONFLUENCE OF LARGE-SCALE SEMICONDUCTOR FABRICATION, MICRO-OPTOMECHANICAL & MICRO-ELECTRO-OPTICAL SYSTEMS AND MACHINE LEARNING

The startups three founders are Nicolas Abelé, Karel Dumon and Clément Javerzac-Galy, respectively.

One thing the startup can rely on is a strong team vision built on the idea of ‘pioneering a sustainable future with photonic and quantum tech’.

Miraex’s technology for sensing and quantum applications using photons instead of electrons full-stack quantum computing solutions includes the Quantum Transducer: ‘microwave to optical’ and the Quantum Converter: ‘preserving quantum states’. These can be used in industry, aerospace, security, defence, and quantum networking solutions and can help clients ‘save energy, avoid accidents or protect their critical assets’.

What’s not to like?

All this comes from the hard work and intelligence of the founding team – so, let’s meet them:

Serial entrepreneur and innovator Nicolas Abelé, the startup’s co-CEO, has years of experience in micro-electro-mechanical (MEMS) system-based optoelectronics and AR display products. With a Ph.D. from EPFL in microsystems engineering, he is also impressively a laureate of the 2005 European Award for Innovation.

Karel Dumon holds an MS in engineering physics from Ghent University. Before co-founding Miraex, Dumon spent time as a business analyst, researcher, data scientist and machine learning engineer while also cofounding two startups.

Sharing co-CEO duties with Abelé is Clément Javerzac-Galy, and like Abelé, Javerzac-Galy has a Ph.D. from EPFL in physics. He has an impressive résumé, too, with stints as an engineering intern at Thales, guest researcher at the Joint Quantum Institute and blogger at Swiss publication Bilan.

So, what’s next for this Swiss QC startup? Well, according to Javerzac-Galy, the answer is simple: “Today we are deploying our solutions in the energy and food sectors and we are preparing to expand to aerospace applications.”

With a strong idea backing up the trio, Miraex can also count on the support of its partnerships which include VC and private equity firm Creative Destruction Lab, Switzerland’s leading seed-funding program Venture Kick (both of which participated in a CHF40,000 grant to Miraex in 2019) and Lausanne-based innovation promotion agency Innovaud amongst others.

13 Fault Tolerance Demonstrated on an Ion Trap Quantum Computer

by Dr. Andre Saraiva

https://quantumcomputingreport.com/its-finally-here-fault-tolerance-demonstrated-on-an-ion-trap-quantum-computer/

Late in June this year, quantum computing Professor Christopher Monroe wrote to Nature describing how COVID-19 restricted access to his lab at University of Maryland. Perhaps unexpectedly, he reported that the remotely controlled experiments his team had set up were delivering 'the best data (they) have ever seen'. This means a lot coming from a group that was already demonstrating extremely high-fidelity operations before the noise levels came down. How much better could their ion-trap-based qubits get?

Now, the anticipation is over. In a preprint manuscript led by Monroe and Marko Cetina from Duke University, they demonstrated the holy grail of large scale quantum computing – fault tolerance. In their own words, this means "an encoded logical qubit whose logical fidelity exceeds the fidelity of the entangling operations used to create it".

While the result has not been peer reviewed yet, this work is a natural consequence of the years of developments incorporated in their architecture. Their quantum computer starts by removing an electron from single ytterbium atoms to turn them into ions that can be trapped above a microfabricated chip inside a vacuum chamber (which is at room temperature). They cool down just the atoms with lasers, obtaining extremely high-quality spin qubits, with coherence times of a few seconds (limited only by fluctuations in magnetic field due to the external magnet).

The recent progress in high quality control tools developed by the group is what made these results possible. Some years ago, they demonstrated individual optical addressability using an acousto-optic modulators (their current quantum computer has 32 channels, so they are ready to do even larger multiqubit experiments in the near future). All-to-all coupling is achieved by converting the spin qubit states into motional states for a brief period (or even only virtually), such that two spin qubits that were set to couple with the collective oscillations will effectively interact with each other. This is called the Mølmer-Sørensen interaction.

Logical qubits are implemented by encoding 0s and 1s on the collective state of several physical qubits. Fault tolerance is then described as the limit when the collective state of the logical qubit outperforms each separate physical qubit – which is not easy to achieve because the more qubits one operates, the higher the probability of introducing an error. But eventually, in the limit of many qubits and many stabilizing operations, fault tolerance should be achievable. They use only 9 qubits in their fault-tolerant logical qubit implementation (what is called a [[9,1,3]] Bacon-Shor code), which is an impressively small set. Another 4 ions are used as ancillas to measure hints of errors in some properties of parts of the logical qubit (called stabilizers).

They also demonstrate a non-fault-tolerant implementation of a "magic state". This is a key resource for implementing universally programmable quantum computers, since it can be used for "distillation", which is how a multiqubit system can access parts of the Hilbert space that make a quantum computer completely non-simulatable by classical computers (beyond the so-called Clifford space).

So, what's next?

Well, many things. The most immediate one is backing up the claims with peer review – which hopefully will not be a problem since this manuscript is already making a lot of noise in the community. Secondly, it is now time to ask how far can this quantum computer go. After all, with only 15 qubits they have demonstrated what Google's 53 qubit system hasn't. And they still have a few channels that they can use.

Now, this does not mean we are done. The error correction code they demonstrated does not have a threshold like the surface code, for example. This means that the more logical qubits one has, the more errors will build up, and eventually this form of encoding qubits will also reach its ceiling. This is true, no matter how accurate each logical qubit may be. The surface code, on the other hand, has a demonstrated threshold – a tipping point at which error correction completely reverts all errors and a long term, large scale computation can be sustained.

25 Sep 2020

14 Boston-based quantum startup Zapata releases Orquestra, a new software platform

by G Jeremy

https://quantumzeitgeist.com/boston-based-quantum-startup-zapata-releases-orquestra-a-new-software-platform/

Despite skeptics having doubts about the 'realness' of the imminent field of quantum computing, there are many strides forward made even now. IBM recently released an ambitious roadmap that is hardware-based, and Zapata, a Boston-based quantum computing startup, announced its commercial release of Orquestra. It is an advanced software platform used to create repeatable quantum and quantum-based workflows and algorithms and can be used across industries and cases. The process involves a quantum engine that systematically groups together information and resources even when they are spread across both quantum and classical devices.

Previously, only Early Access participants could use Orquestra, but it is now able to be integrated with IBM, Amazon Bracket (which provides access to simulators), IonQ, Rigetti, and Honeywell's System Model HØ. It is the first platform to allow value-added access to Honeywell's system, which means that users can now directly run quantum workflows on the Honeywell machine.

> Orquestra gives us the opportunity to make bigger projects tractable.
>
> – Professor of Quantum Information Science

Orquestra is designed for quantum use cases such as writing, manipulating, and optimising quantum circuits as well as running these across various devices. These devices include quantum computers, simulators, and HPC resources. Orquestra provides the following functions:

Optimised open-source and exclusive algorithms can be supplied by extensive quantum algorithm repositories. Code can be combined by users from various different quantum libraries for workflow management systems. Many different quantum and classical backends can be run and benchmarked.

> It is amazing to finally use the Honeywell system directly through Orquestra. The algorithms we are working with are complex, to say the least, and running them through Orquestra on real quantum devices is game-changing.
>
> – BP, user of Orquestra

15 Baidu Announces Cloud-Based Quantum Computing Platform

by Matt Swayne

https://thequantumdaily.com/2020/09/25/baidu-announces-cloud-based-quantum-computing-platform/

China-based Baidu Inc. announced in a blog post that it has released a new cloud-based quantum computing platform called **Quantum Leaf** that is designed for programming, simulating and executing quantum workloads.

The company added the cloud-based QC platform is aimed at providing the quantum programming environment for Quantum infrastructure as a Service (QaaS).

In May, Baidu Quantum Computing Institute announced Paddle Quantum, a quantum machine learning development toolkit based on PaddlePaddle that can help scientists and developers quickly build and train quantum neural network models and provide advanced quantum computing applications.

A key component in the Quantum Leaf architecture is QCompute, a Python-based open-source SDK. It provides a full-stack programming experience for advanced users via the features of hybrid quantum programming language and a high-performance simulator. Users can use the already-built objects and modules of quantum programming environment, pass parameters to build and execute the quantum circuits on the local simulator or the cloud simulator/hardware.

QCompute provides services for creating and analyzing quantum circuits and calling quantum backend.

In addition to Paddle Quantum and Quantum Leaf, the company also reported it developed a cloud-based quantum pulse computing service named **Quanlse**, which aims to bridge the gap between quantum software and hardware. With Quanlse, Paddle Quantum, and Quantum Leaf, Baidu Quantum Platform moves further to its mission "Everyone Can Quantum."

The original announcement came at the company's user conference, Baidu World 2020.

16 Spin clean-up method brings practical quantum computers closer to reality

by Osaka City University

https://phys.org/news/2020-09-clean-up-method-quantum-closer-reality.html

Quantum computers are the new frontier in advanced research technology, with potential applications such as performing critical calculations, protecting financial assets, or predicting molecular behavior in pharmaceuticals. Researchers from Osaka City University have now solved a major problem hindering large-scale quantum computers from practical use: precise and accurate predictions of atomic and molecular behavior.

They published their method to remove extraneous information from quantum chemical calculations on Sept. 17 as an advanced online article in Physical Chemistry Chemical Physics, a journal of the Royal Society of Chemistry.

"One of the most anticipated applications of quantum computers is electronic structure simulations of atoms and molecules," said paper authors Kenji Sugisaki, Lecturer and Takeji Takui, Professor Emeritus in the Department of Chemistry and Molecular Materials Science in Osaka City University's Graduate School of Science.

Quantum chemical calculations are ubiquitous across scientific disciplines, including pharmaceutical therapy development and materials research. All of the calculations are based on solving physicist Erwin Schrödinger's equation, which uses electronic and molecular interactions that result in a particular property to describe the state of a quantum-mechanical system.

"Schrödinger equations govern any behavior of electrons in molecules, including all chemical properties of molecules and materials, including chemical reactions," Sugisaki and Takui said.

On classical computers, such precise equations would take exponential time. On quantum computers, this precision is possible in realistic time, but it requires "cleaning" during the calculations to obtain the true nature of the system, according to them.

A quantum system at a specific moment in time, known as a wave function, has a property described as spin, which is the total of the spin of each electron in the system. Due to hardware faults or mathematical errors, there may be incorrect spins informing the system's spin calculation. To remove these 'spin contaminants,' the researchers implemented an algorithm that allows them to select the desired spin quantum number. This purifies the spin, removing contaminants during each calculation – a first on quantum computers, according to them.

"Quantum chemical calculations based on exactly solving Schrödinger equations for any behavior of atoms and molecules can afford predictions of their physical-chemical properties and complete interpretations on chemical reactions and processes," they said, noting that this is not possible with currently available classical computers and algorithms. "The present paper has given a solution by implementing a quantum algorithm on quantum computers."

The researchers next plan to develop and implement algorithms designed to determine the state of electrons in molecules with the same accuracy for both excited- or ground-state electrons.

24 Sep 2020

17 Zapata Announces Commercial Release of Orquestra

by Zapata Computing

http://www.globenewswire.com/news-release/2020/09/24/2098623/0/en/Zapata-Announces-Commercial-Release-of-Orquestra-the-Workflow-Based-Modular-Toolset-for-Applied-Quantum-C
html

Zapata Computing, a leading enterprise software company for quantum computing, today announced the commercial release of **Orquestra**, a workflow-based, unified toolset for applied quantum computing that allows users to compose and run quantum workflows across a range of devices, both quantum and classical, on a unified quantum operating environment. Previously accessible only to Early Access Program participants, Orquestra is now commercially available as a highly extensive workflow management tool for developing quantum and quantum-inspired workflows and algorithms across use cases and industries.

"The Orquestra Early Access Program allowed enterprise and academic teams to manage their complex mix of use cases, devices and approaches to application development by coordinating everything from systems preparation to data analysis," says Christopher Savoie, CEO and co-founder of Zapata. "By leveraging Orquestra's workflow-based systems for real customer applications, we were able to accelerate their work significantly. Their usage and feedback have also fueled major improvements to Orquestra's features, integrations and interactions."

18 New system detects faint communications signals using the principles of quantum physics

by NIST

https://phys.org/news/2020-09-faint-principles-quantum-physics.html

Researchers at the National Institute of Standards and Technology (NIST) have devised and demonstrated a system that could dramatically increase the performance of communications networks while enabling record-low error rates in detecting even the faintest of signals, potentially decreasing the total amount of energy required for state-of-the-art networks by a factor of 10 to 100.

The proof-of-principle system consists of a novel receiver and corresponding signal-processing technique that, unlike the methods used in today's networks, are entirely based on the properties of quantum physics and thereby capable of handling even extremely weak signals with pulses that carry many bits of data.

"We built the communication test bed using off-the-shelf components to demonstrate that quantum-measurement-enabled communication can potentially be scaled up for widespread commercial use," said Ivan Burenkov, a physicist at the Joint Quantum Institute, a research partnership between NIST and the University of Maryland. Burenkov and his colleagues report the results in Physical Review X Quantum. "Our effort shows that quantum measurements other valuable, heretofore unforeseen advantages for telecommunications leading to revolutionary improvements in channel bandwidth and energy efficiency."

Modern communications systems work by converting information into a laser-generated stream of digital light pulses in which information is encoded – in the form of changes to the properties of the light waves – for transfer and then decoded when it reaches the receiver. The train of pulses grows fainter as it travels along transmission channels, and conventional electronic technology for receiving and decoding data has reached the limit of its ability to precisely detect the information in such attenuated signals.

The signal pulse can dwindle until it is as weak as a few photons – or even less than one on average. At that point, inevitable random quantum fluctuations called "shot noise" make accurate reception impossible by normal ("classical," as opposed to quantum) technology because the uncertainty caused by the noise makes up such a large part of the diminished signal. As a result, existing systems must amplify the signals repeatedly along the transmission line, at considerable energy cost, keeping them strong enough to detect reliably.

The NIST team's system can eliminate the need for amplifiers because it can reliably process even extremely feeble signal pulses: "The total energy required to transmit one bit becomes a fundamental factor hindering the development of networks," said Sergey Polyakov, senior scientist on the NIST team. "The goal is to reduce the sum of energy required by lasers, amplifiers, detectors, and support equipment to reliably transmit information over longer distances. In our work here we demonstrated that with the help of quantum measurement even faint laser pulses can be used to communicate multiple bits of information – a necessary step towards this goal."

To increase the rate at which information can be transmitted, network researchers are finding ways to encode more information per pulse by using additional properties of the light wave. So a single laser light pulse, depending on how it was originally prepared for transmission, can carry multiple bits of data. To improve detection accuracy, quantum-enhanced receivers can be fitted onto classical network systems. To date, those hybrid combinations can process up to two bits per pulse. The NIST quantum system uses up to 16 distinct laser pulses to encode as many as four bits.

To demonstrate that capability, the NIST researchers created an input of faint laser pulses comparable to a substantially attenuated conventional network signal, with the average number of photons per pulse from 0.5 to 20 (though photons are whole particles, a number less than one simply means that some pulses contain no photons).

After preparing this input signal, the NIST researchers take advantage of its wavelike properties, such as interference, until it finally hits the detector as photons (particles). In the realm of quantum physics, light can act as either particles (photons) or waves, with properties such as frequency and phase (the relative positions of the wave peaks).

Inside the receiver, the input signal's pulse train combines (interferes) with a separate, adjustable reference laser beam, which controls the frequency and phase of the combined light stream. It is extremely difficult to read the different encoded states in such a faint signal. So the NIST system is designed to measure the properties of the whole signal pulse by trying to match the properties of the reference laser to it exactly. The researchers achieve this through a series of successive measurements of the signal, each of which increases the probability of an accurate match.

That is done by adjusting the frequency and phase of the reference pulse so that it interferes destructively with the signal when they are combined at the beam splitter, canceling the signal out completely so no photons can be detected. In this scheme, shot noise is not a factor: Total cancelation has no uncertainty.

Thus, counterintuitively, a perfectly accurate measurement results in no photon reaching the detector. If the reference pulse has the wrong frequency, a photon can reach the detector. The receiver uses the time of that photon detection to predict the most probable signal frequency and adjusts the frequency of the reference pulse accordingly. If that prediction is still incorrect, the detection time of the next photon results in a more accurate prediction based on both photon detection times, and so on.

"Once the signal interacts with the reference beam, the probability of detecting a photon varies in time," Burenkov said, "and consequently the photon detection times contain information about the input state. We use that information to maximize the chance to guess correctly after the very first photon detection.

"Our communication protocol is designed to give different temporal profiles for different combinations of the signal and reference light. Then the detection time can be used to distinguish between the input states with some certainty. The certainty can be quite low at the beginning, but it is improved throughout the measurement. We want to switch the reference pulse to the right state after the very first photon detection because the signal contains just a few photons, and the longer we measure the signal with the correct reference, the better our confidence in the result is."

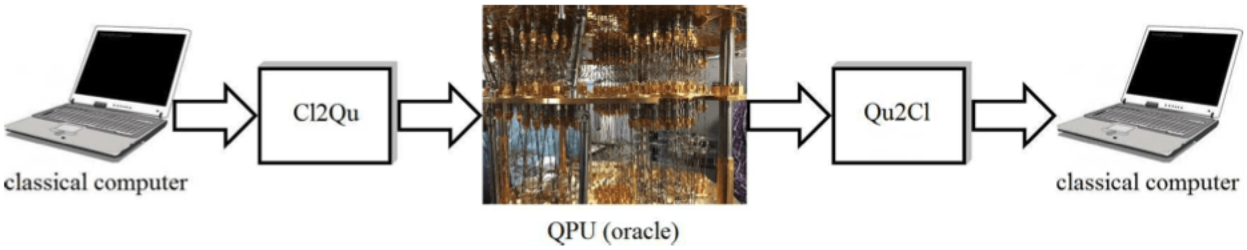
Polyakov discussed the possible applications. "The future exponential growth of the internet will require a paradigm shift in the technology behind communications," he said. "Quantum measurement could become this new technology. We demonstrated record low error rates with a new quantum receiver paired with the optimal encoding protocol. Our approach could significantly reduce energy for telecommunications."

22 Sep 2020

19 Internal representation of a digital image inside a quantum processor

https://www.swissquantumhub.com/internal-representation-of-a-digital-image-inside-a-quantum-processor/

Scientists at Florida International University have compared five techniques for the representation of a digital image inside a quantum processor.



Since its inception nearly two decades ago, Quantum Image Processing (QImP) has always dealt with the same problem, i.e., the internal representation of a digital image inside a quantum circuit efficiently, where such circuits can be optical or of superconductors. In the case of superconducting quantum platforms, they have been freely available to the entire scientific community for approximately five years, which has allowed testing the different techniques for the internal representation of an image on a real physical machine without the need for theoretical speculations. However, during the last five years we have witnessed a complete absence of such implementations.

From all the accumulated experience in Quantum Information Processing, the scientific community knows that the problem with simulators is that they represent a necessary but not sufficient condition, i.e., if something works in a simulator, e.g. Qiskit, it still needs to be tested on a QPU, but if something does not work in a simulator, then do not even bother to move to the QPU because it is clear that our quantum algorithm under test has problems.

The techniques are: flexible representation of quantum images (FRQI), novel enhanced quantum representation (NEQR), generalized quantum image representation (GQIR), multi-channel representation for quantum images (MCQI), and quantum Boolean image processing (QBIP).

The comparison has been based on implementations on the Quirk simulator, and on the IBM Q Experience processors, from the point of view of performance, robustness (noise immunity), deterioration of the outcomes due to decoherence, and technical viability.

21 Sep 2020

20 Hearsay Around Chinese Quantum Supremacy

by Dr. Andre Saraiva

https://quantumcomputingreport.com/hearsay-around-chinese-quantum-supremacy/

The achievements of Chinese academician Jianwei Pan have earned him the nickname of “**Father of Quantum**” in the Chinese scientific community. His success history recently culminated in the first quantum satellite, which distributes entangled photons between ground and an orbit thousands of kilometres high. His reputation explains why the scientific community got so hastily excited when rumours spread about his 50-photon boson sampling quantum computer, which would potentially outperform Google's Sycamore quantum processor in a quantum supremacy experiment.

The English-language publication South China Morning Post reported that Jianwei Pan "announced at a lecture at Westlake University, Hangzhou, on September 5, 2020 that a new machine had recently achieved "quantum supremacy" one million times greater than the record currently held by Sycamore". This claim is currently not supported by any publication, so it is unclear what is the exact meaning of a "greater supremacy", but it is probably related to the notoriously large dimension spanned by the states achieved in boson sampling devices.

The USTC (University of Science and Technology of China) team led by Pan was fast to communicate through the Chinese social media Weibo that they worry about the claim of potential quantum supremacy being quoted out of context. Indeed, the scientific community customarily goes by the motto "extraordinary claims require extraordinary evidence" – especially when it comes to quantum computing, in which inflated claims can turn into money flow. But Pan's team has already shown progress in this direction last year, when a 20-photon boson sampling quantum computer was demonstrated. Moreover, Jianwei Pan co-signs a preprint manuscript dedicated to the benchmarking of a – at this point hypothetical – 50 photon boson sampling quantum computer against China's classical supercomputer Sunway Taihulight.

The claim of "'quantum supremacy' So, what's next? one million times greater" than Google's experiment does not raise much skepticism, though. In the game of quantum advantage, gain is typically exponential. A handful of additional qubits can already give a quantum computer six orders of magnitude increase in computational power, whatever the metrics for this Pan's group might be proposing. But in this case, their boson sampling system is doing precisely what it was designed to achieve.

Boson sampling was proposed as a simplified version of linear optics quantum computers. The general-purpose version of linear optical quantum computers, called the KLM architecture after its inventors Knill, Laflamme and Milburn, is much harder to implement and will only start giving out results at the mark of millions of photonic qubits. On the other hand, boson sampling can already outperform classical computers in a specific task at only tens of single photon modes.

Notice, though, the use of the term "single photon modes", as opposed to qubits. This is because boson sampling architectures are not like other quantum computers based on qubits and logical gate operations. Boson sampling is based, instead, on the capacity of a collective multimode photon system to map complicated statistical distributions that are hard to obtain with a classical computer.

This means that there are two shortcomings for the boson sampling quantum computer. Firstly, it is believed to be inherently purpose-specific since there is no well-defined way to convert arbitrary algorithms into the boson sampling problem. That means that this quantum computer has no perspective to run famed algorithms such as Shor's factorisation or Grover's search algorithm.

Moreover, only a handful of real-life problems of interest have been theoretically demonstrated to be solvable in a boson sampling quantum computer. This severely limits the market for these devices when compared to the quantum computing model of traditional universal quantum computers. Current examples of application of boson sampling include the calculation of vibronic spectra of molecules, solving some spin Hamiltonians and problems in graph identification.

From a fundamental point of view, however, this demonstration is extremely valuable. It may serve, for instance, to experimentally probe the limits of the extended Church-Turing thesis which states that a universal computing device can simulate every physical process. A boson sampling device could be the first counterexample disproving this thesis. And this seemingly philosophical question can only be answered in the context of cold hard quantum error analysis. That is because the boson sampling problem is only computationally hard (#P-hard, to be more precise, which is a harder class than NP-complete) if error rates grow less than polynomially with the number of input photons.

While most naïve models of error actually predict an exponentially increasing error rate, Jianwei Pan's team will finally be able to quantitatively analyse this effect and exactly up to which point is the boson sampling supremacy as astounding as predicted. The technical aspects of their photonic system from last year were already at the cutting edge in all parts: a single quantum dot is resonantly coupled to a microcavity creating single photons, which are demultiplexed into a stream of photon pulses into 20 spatial modes. The 20 input single photons were injected into a 3D integrated, 60-mode ultra-low-loss photonic circuit. Finally, the output single photons are detected by 60 superconducting nanowire single-photon detectors with coincidences recorded in a 64-channel coincidence count unit.

So, what's next?

Well, firstly we need to see proof that this result was really obtained by the Chinese researchers. But assuming that Jianwei Pan's team has the data to back up his claim, then this should serve as a major push for further research into the possible applications of boson sampling. After Google's supremacy demonstration on a gate-based programmable superconducting quantum processor, the mere demonstration of supremacy is no longer such a high prize. Pan's team may need to focus on more extravagant displays of strength in order to keep happy the deep-pocketed Chinese funding agencies.

21 Critical Zerologon bug uses weak cryptography to spoof network users

by Derek B. Johnson

https://www.scmagazine.com/home/security-news/vulnerabilities/critical-zerologon-bug-uses-weak-cryptography-to-spoof-network-users/

Organizations should prioritize patching over detection when it comes to **Zerologon**, a recently disclosed privilege escalation vulnerability in Microsoft's Windows server operating system.

The bug, which received a 10 out of 10 for severity by the Common Vulnerability Scoring System, exploits a flaw in the customized cryptographic protocol used by Netlogon to authenticate communications between a client and Windows domain server and update passwords.

In short, the attacker can spoof any computer or person on a network by leveraging weaknesses in Netlogon's custom encryption protocol when a Windows server domain attempts to authenticate the client's identity. This is because in certain instances when Netlogon uses the default AES encryption to generate a session key, it creates an Initialization Vector value made up of all zeros. For every 256 keys generated, researchers found that one on average will result in an all-zero ciphertext. Since there's no limit on the number of invalid login attempts a client can make, an impersonator on the network could easily brute force challenges to the server over and over again until the parties settle on an all-zero key.

Tom Tervoort, a security researcher at Secura, noted that it only takes an attacker a few seconds to cycle through those 256 attempts until they get a key composed of all zeroes. From there, they can disable other security protocols like RPC signing and sealing, change the domain controller password and even gain admin privileges across an enterprise.

“This attack has a huge impact: it basically allows any attacker on the local network (such as a malicious insider or someone who simply plugged in a device to an on-premise network port) to completely compromise the Windows domain,” wrote Tervoort in a technical whitepaper on the flaw.

Adam Meyers, vice president of intelligence at CrowdStrike, told SC Media that an attacker would need to have an initial foothold into a victim network first – likely through commodity malware or a successful phishing attack – before exploiting the bug. But those who do have that access can substantially reduce their breakout time before moving laterally and compromising other systems and devices. Ransomware actors and other cyber criminals could find it a particularly attractive option to escalate their privileges across a network and deploy their payload before an organization even knows what hit them.

“This is something that will change the calculus of how fast an adversary can move,” he said.

Organizations across the public and private sector are moving to sound the alarm. Late Friday night, the Cybersecurity and Infrastructure Security Agency issued an emergency directive ordering civilian federal agencies to immediately patch or disable all affected Windows servers, and warned non-governmental organizations to do the same.

“Although the Emergency Directive only applies to . . . federal agencies, we strongly recommend that state and local government, the private sector, and the American public also apply this security update as soon as possible,” the agency tweeted out shortly after the directive was released.

Two organizations – including Secura – have already developed and released Proof of Concept code, and Meyers said it will soon be incorporated into open source tools like Mimikatz that are a staple for many criminal hacker groups.

As a result, organizations should be focused on immediately updating to the latest operating system as opposed to setting up detection protocols, though that can also provide situational awareness and help identify an attacker on your network trying to exploit the flaw. Thankfully, Microsoft already issued a patch in August that allows Domain Controllers to protect Windows devices by default, and also adds new protections by logging any suspicious or warning events for vulnerable devices across the domain. A second patch will require all Windows and non-Windows devices to use secure Remote Procedure Call with Netlogon, but Microsoft is pushing that update until first quarter of 2021 to allow some vendors time to work out implementation issues.

Still, experts advise companies to move fast implementing the initial update.

“I think this is one of the [vulnerabilities] that is highly likely to be used by threat actors now, so I would not spend a lot of time waiting to patch,” said Meyers.

22 Your data isn’t safe until your crypto keys are safe

by Peter Carlisle

https://www.itproportal.com/features/your-data-isnt-safe-until-your-crypto-keys-are-safe/

As all CIOs and IT managers know, data security is a continual process. As your security changes, so does the threat. For example, if you have encrypted your corporate data then your business secrets can’t be intercepted. Lost devices containing sensitive information are unreadable. Now, the threat has moved to your crypto key. Is it as safe as it needs to be? Here we explain the importance of protecting your key by looking at the methods that hackers use to circumvent encryption.

Businesses encrypt data for a number of reasons: to protect corporate secrets, to safeguard customers' personal information to comply with regulations, and to maintain customer trust and goodwill. IT pros are all too aware that their data is vulnerable to attack and that encryption is one of the best security and data protection tools available. It's listed within Article 32 of the GDPR as an appropriate technical and organizational measure to ensure data security, depending on the nature and risks of your processing activities. The Information Commissioner's Office (ICO) advises its use when storing or transmitting personal data and certain sector-specific regulations go further and actually require encryption. For example, the banking industry's Payment Card Industry Data Security Standard (PCI DSS) requires businesses accepting card payments to use certain TLS (Transport Layer Security) cryptographic handshake protocols for data in transit.

While the cost of losing business secrets is harder to quantify – and may be immeasurably large, even fatal to a business – financial penalties for customer data breaches can be estimated. Although the GDPR contains no explicit fine associated with not implementing encryption, encryption may protect organizations from fines related to data breach. In one of the largest fines handed out to date, Marriott International Hotels was ordered to pay 110.3M Euros to the ICO in the UK after a hack of its systems exposed sensitive personal information including credit card details, passport numbers, as well as dates of birth belonging to over 300 million clients of which 30 million were EU residents.

Moving into the quantum age

While regulations and headline fines have convinced businesses of the need for encryption, the message on key security hasn't been as loud. One of today's data protection challenges is that while most security professionals understand the strength of standardized encryption through peer vetting, they are not so aware of the singular importance of keeping the key protected. Today's popular cryptographic algorithms like ECC, AES, 3DES and RSA are well documented and well tested. They work because of the unique and complex keys that they generate. A 256 bit AES key – the standard used by the US government – has 1.15×10^{77} possible combinations. With current computing power, the time needed to decrypt protected data is measured in millions of years. Looked at another way, encryption processes are now so strong that they make the key the Achilles heel.

Even considering future computing power, the key will be the vulnerable part of encryption. As we move to a quantum computing age, the first post-quantum cryptography standard will close the door to hackers using quantum computing to strong-arm encrypted data. There is a risk that when quantum computing becomes available to hackers all data encrypted with current keys will be unprotected. As the National Institute of Standards and Technology (NIST) says in a recent report, "when that day comes, all secret and private keys that are protected using the current public-key algorithms – and all available information protected under those keys – will be subject to exposure." Our industry is already working on larger signatures and key sizes (for example using message segmentation) to meet the challenge.

Storing keys securely

Assuming then that hackers will make stealing a crypto key a priority, how could they do it? One known way is finding the key stored in software on your network. If a key is stored in this way then it is vulnerable to theft. A crypto key can be recognized in a binary scan, using relatively unsophisticated programs. It will appear as a randomized pattern that the intruder will know means they have hit the jackpot. While they don't have millions of years to brute force encrypted data, they will have the time it takes to test keys against your data. Based on a number of studies, the time between a hacker's penetration and detection is between 160 and 260 days. Even at the low end, that's a large number of hours. A company is likely to have only a few thousand keys, a number low enough for a hacker to work through.

The way to protect the key, and therefore your data, is to store it in a secure way. A hardware security module (HSM) is a physical computing device to do just that. Its function is to safeguard and manage digital keys and perform other cryptographic functions. A HSM is designed using strict standards developed by NIST precisely to provide the final layer of security in data encryption. Unlike storing a key in software, which isn't subject to any standards, and where it could be copied or stolen, the HSM gives you control over key access. It stays in the HSM. For some industries like the payment card industry a HSM is a way for businesses to comply with the data security standards they need to meet in order to operate. For other businesses, using a HSM shows that they are serious about customer and corporate data.

To encrypt without protecting your key is to fail at the final and most important hurdle of data security. It's the digital world version of locking your doors and then leaving your key under a plant pot. A smart burglar will look there, and a hacker who sees encrypted data will look in every possible hiding place on your system for your keys. The rewards will be worth it for them. Until your crypto key is safe, your data isn't safe.

19 Sep 2020

23 Set of two-qubit gates for near-term quantum algorithms

https://www.swissquantumhub.com/set-of-two-qubit-gates-for-near-term-quantum-algorithms/

Quantum algorithms offer a dramatic speedup for computational problems in material science and chemistry. However, any near-term realizations of these algorithms will need to be optimized to fit within the finite resources offered by existing noisy hardware.

Here, taking advantage of the adjustable coupling of gmon qubits, researchers demonstrated a continuous two-qubit gate set that can provide a threefold reduction in circuit depth as compared to a standard decomposition.

They implemented two gate families: an imaginary swap-like (iSWAP-like) gate to attain an arbitrary swap angle, θ, and a controlled-phase gate that generates an arbitrary conditional phase, ϕ.

Using one of each of these gates, they were able to perform an arbitrary two-qubit gate within the excitation-preserving subspace allowing for a complete implementation of the so-called Fermionic simulation (fSim) gate set.

24 Revolutionary Quantum Cryptography Breakthrough Paves Way for Safer Online Communication

by UNIVERSITY OF BRISTOL

https://scitechdaily.com/revolutionary-quantum-cryptography-breakthrough-paves-way-for-safer-online-communication/

The world is one step closer to having a totally secure internet and an answer to the growing threat of cyber-attacks, thanks to a team of international scientists who have created a unique prototype that could transform how we communicate online.

The invention led by the University of Bristol, revealed today in the journal Science Advances, has the potential to serve millions of users, is understood to be the largest-ever quantum network of its kind, and could be used to secure people's online communication, particularly in these internet-led times accelerated by the COVID-19 pandemic.

By deploying a new technique, harnessing the simple laws of physics, it can make messages completely safe from interception while also overcoming major challenges that have previously limited advances in this little used but much-hyped technology.

Lead author Dr. Siddarth Joshi, who headed the project at the university's Quantum Engineering Technology (QET) Labs, said: "This represents a massive breakthrough and makes the quantum internet a much more realistic proposition. Until now, building a quantum network has entailed huge cost, time, and resource, as well as often compromising on its security which defeats the whole purpose."

"Our solution is scalable, relatively cheap and, most important of all, impregnable. That means it's an exciting game changer and paves the way for much more rapid development and widespread rollout of this technology."

The current internet relies on complex codes to protect information, but hackers are increasingly adept at outsmarting such systems leading to cyber-attacks across the world which cause major privacy breaches and fraud running into trillions of pounds annually. With such costs projected to rise dramatically, the case for finding an alternative is even more compelling and quantum has for decades been hailed as the revolutionary replacement to standard encryption techniques.

So far physicists have developed a form of secure encryption, known as quantum key distribution, in which particles of light, called photons, are transmitted. The process allows two parties to share, without risk of interception, a secret key used to encrypt and decrypt information. But to date this technique has only been effective between two users.

"Until now efforts to expand the network have involved vast infrastructure and a system which requires the creation of another transmitter and receiver for every additional user. Sharing messages in this way, known as trusted nodes, is just not good enough because it uses so much extra hardware that could leak and would no longer be totally secure," Dr. Joshi said.

The team's quantum technique applies a seemingly magical principle, called entanglement, which Albert Einstein described as 'spooky action at a distance.' It exploits the power of two different particles placed in separate locations, potentially thousands of miles apart, to simultaneously mimic each other. This process presents far greater opportunities for quantum computers, sensors, and information processing.

"Instead of having to replicate the whole communication system, this latest methodology, called multiplexing, splits the light particles, emitted by a single system, so they can be received by multiple users efficiently," Dr. Joshi said.

The team created a network for eight users using just eight receiver boxes, whereas the former method would need the number of users multiplied many times – in this case, amounting to 56 boxes. As the user numbers grow, the logistics become increasingly unviable – for instance 100 users would take 9,900 receiver boxes.

To demonstrate its functionality across distance, the receiver boxes were connected to optical fibers via different locations across Bristol and the ability to transmit messages via quantum communication was tested using the city's existing optical fiber network.

"Besides being completely secure, the beauty of this new technique is its streamline agility, which requires minimal hardware because it integrates with existing technology," Dr. Joshi said.

The team's unique system also features traffic management, delivering better network control which allows, for instance, certain users to be prioritized with a faster connection.

Whereas previous quantum systems have taken years to build, at a cost of millions or even billions of pounds, this network was created within months for less than £300,000. The financial advantages grow as the network expands, so while 100 users on previous quantum systems might cost in the region of £5 billion, Dr. Joshi believes multiplexing technology could slash that to around £4.5 million, less than 1 percent.

In recent years quantum cryptography has been successfully used to protect transactions between banking centers in China and secure votes at a Swiss election. Yet its wider application has been held back by the sheer scale of resources and costs involved.

"With these economies of scale, the prospect of a quantum internet for universal usage is much less far-fetched. We have proved the concept and by further refining our multiplexing methods to optimize and share resources in the network, we could be looking at serving not just hundreds or thousands, but potentially millions of users in the not too distant future," Dr. Joshi said.

"The ramifications of the COVID-19 pandemic have not only shown importance and potential of the internet, and our growing dependence on it, but also how its absolute security is paramount. Multiplexing entanglement could hold the vital key to making this security a much-needed reality.

18 Sep 2020

25 New design principles for spin-based quantum materials

by Northwestern University

https://www.sciencedaily.com/releases/2020/09/200918122207.htm

As our lives become increasingly intertwined with technology – whether supporting communication while working remotely or streaming our favorite show – so too does our reliance on the data these devices create. Data centers supporting these technology ecosystems produce a significant carbon footprint – and consume 200 terawatt hours of energy each year, greater than the annual energy consumption of Iran. To balance ecological concerns yet meet growing demand, advances in microelectronic processors – the backbone of many Internet of Things (IoT) devices and data hubs – must be efficient and environmentally friendly.

Northwestern University materials scientists have developed new design principles that could help spur development of future quantum materials used to advance (IoT) devices and other resource-intensive technologies while limiting ecological damage.

"New path-breaking materials and computing paradigms are required to make data centers more energy-lean in the future," said James Rondinelli, professor of materials science and engineering and the Morris E. Fine Professor in Materials and Manufacturing at the McCormick School of Engineering, who led the research.

The study marks an important step in Rondinelli's efforts to create new materials that are non-volatile, energy efficient, and generate less heat – important aspects of future ultrafast, low-power electronics and quantum computers that can help meet the world's growing demand for data.

Rather than certain classes of semiconductors using the electron's charge in transistors to power computing, solid-state spin-based materials utilize the electron's spin and have the potential to support low-energy memory devices. In particular, materials with a high-quality persistent spin texture (PST) can exhibit a long-lived persistent spin helix (PSH), which can be used to track or control the spin-based information in a transistor.

Although many spin-based materials already encode information using spins, that information can be corrupted as the spins propagate in the active portion of the transistor. The researchers' novel PST protects that spin information in helix form, making it a potential platform where ultralow energy and ultrafast spin-based logic and memory devices operate.

The research team used quantum-mechanical models and computational methods to develop a framework to identify and assess the spin textures in a group of non-centrosymmetric crystalline materials. The ability to control and optimize the spin lifetimes and transport properties in these materials is vital to realizing the future of quantum microelectronic devices that operate with low energy consumption.

"The limiting characteristic of spin-based computing is the difficulty in attaining both long-lived and fully controllable spins from conventional semiconductor and magnetic materials," Rondinelli said. "Our study will help future theoretical and experimental efforts aimed at controlling spins in otherwise nonmagnetic materials to meet future scaling and economic demands."

Rondinelli's framework used microscopic effective models and group theory to identify three materials design criteria that would produce useful spin textures: carrier density, the number of electrons propagating through an effective magnetic field, Rashba anisotropy, the ratio between intrinsic spin-orbit coupling parameters of the materials, and momentum space occupation, the PST region active in the electronic band structure. These features were then assessed using quantum-mechanical simulations to discover high-performing PSHs in a range of oxide-based materials.

The researchers used these principles and numerical solutions to a series of differential spin-diffusion equations to assess the spin texture of each material and predict the spin lifetimes for the helix in the strong spin-orbit coupling limit. They also found they could adjust and improve the PST performance using atomic distortions at the picoscale. The group determined an optimal PST material, Sr3Hf2O7, which showed a substantially longer spin lifetime for the helix than in any previously reported material.

"Our approach provides a unique chemistry-agnostic strategy to discover, identify, and assess symmetry-protected persistent spin textures in quantum materials using intrinsic and extrinsic criteria," Rondinelli said. "We proposed a way to expand the number of space groups hosting a PST, which may serve as a reservoir from which to design future PST materials, and found yet another use for ferroelectric oxides – compounds with a spontaneous electrical polarization. Our work also will help guide experimental efforts aimed at implementing the materials in real device structures."

26 Huge threat to national security as hackers attack NIC computers, steal sensitive information

by Neeraj Gaur

https://www.dnaindia.com/india/report-huge-threat-to-national-security-as-hackers-attack-nic-computers-steal-sensitive-information-2843726

In a major development, India's largest data agency National Informatics Centre (NIC) faced a cyberattack in which many computers of the agency were targeted and sensitive information was stolen from them.

The Special Cell of Delhi Police has registered a case and started investigations in connection with this attack.

The NIC contains information related to the national interest, including the Prime Minister and the NSA, among others. In such a situation, this cyber attack is being considered very dangerous. According to the information, this cyberattack has been done by a Bangalore based firm, with connections to the United States

27 What classic software developers need to know about quantum computing

by Bill Detwiler

https://www.techrepublic.com/article/what-classic-software-developers-need-to-know-about-quantum-computing/

IBM, Intel, Google, D-Wave and others have made significant advancements in the field of Quantum computing over the past few years, but many hurdles (not all of them technical) exist before the technology can become a practical alternative for businesses. For example, software developers will need to learn new ways of writing programs for quantum computers.

In May this year, IBM hosted its fourth annual Quantum Challenge. The four-day event consisted of four exercises designed to help classic software developers, researchers, and even business users better understand how quantum programming works. Participants were able to use the 18 IBM Quantum systems on the IBM Cloud to complete the exercises and according to IBM during the event the total use of these system "exceeded 1 billion circuits a day." Over 1,745 people from 45 countries participated in the challenge and 574 people actually completed all four exercises.

In this installment of Dynamic Developer , I talked with one of the IBM team members who helped put the challenge together. In our conversation, Abe Asfaw, Global Lead, Quantum Education and Open Science at IBM, explain the 2020 Quantum Challenge and the challenges developers face when trying to write programs for quantum computers.

⋮

28 Cambridge Quantum Computing with IBM Launches 1st Cloud-Based Quantum Random Number Generator

by Doug Black

https://insidehpc.com/2020/09/cambridge-quantum-computing-with-ibm-launches-1st-cloud-based-quantum-random-number-generator/#:~:text=Random%20Number%20Generator-,Cambridge%20Quantum%20Computing%20with%20IBM%20Launches%201st,Based%20Quantum%20Random%20Number%20Generator&text=Cambridge%20Quantum%20Computing%20(CQC)%20has,integrated%20verification%20for%20the%20user.

Cambridge Quantum Computing (CQC) has launched the world's first cloud-based Quantum Random Number Generation (QRNG) Service with integrated verification for the user.

Randomness is an essential and ubiquitous raw material in almost all digital interactions and is also used in cybersecurity to encrypt data and communications and perform simulation analysis across many sectors, including the petrochemical, pharmaceutical, chemical engineering, finance and gaming industries.

The application developed by CQC generates true maximal randomness, or entropy, implemented on an IBM Quantum Computer that can be verified and thus certified as truly quantum – and therefore truly and maximally random – for the first time. This cannot be accomplished on a classical computer.

As part of a joint effort with IBM, the beta certifiable Quantum Random Number Generation ("cQRNG") Service, which is the first quantum computing application, will initially be available to members of the IBM Q Network, a community of more than 100 Fortune 500 companies, academic institutions, startups and national research labs working with IBM to advance quantum computing.

CQC's IBM partner lead, Anthony Annunziata, Director of the IBM Q Network, provided the following perspective on the new cQRNG Service: "This is an exciting step toward making quantum computers practical and useful, and we are looking forward to seeing what scientists and developers can create using this service."

Working with IBM, CQC has attained two quantum computing milestones: one in computational terms and the other in the commercialization of quantum computing where, for the first time, with the cloud delivery of an application for quantum computers, we provide a service that has real-world application today.

From classical and post-quantum cryptography to complex Monte Carlo simulations where vast amounts of entropy are required to eliminate hidden patterns, certifiable quantum randomness will provide a new opportunity for advantage in relevant enterprise and government applications.

Extracting verified random numbers from a quantum processor has been an industry aspiration for many years. Many current methods only generate pseudo-random numbers or rely on physical phenomena that appear random but are not demonstrably so.

The certified QRNG service launched in partnership with IBM, integrates a Bell test based on Mermin inequalities, offered through the Qiskit module qiskit_rng, which validates the true quantum nature of the underlying processes with statistical analysis. A scientific paper detailing CQC's research titled "Practical Randomness and Privacy Amplification" has been published here.

Lawrence Gasman, president of Inside Quantum Technology, a leading industry research and analysis firm, provided us with this perspective regarding the service: "Certified QRNG is a potentially massive market because there are so many applications of the technology that are possible today, including telecommunications, finance, science and more. Cybersecurity in particular is a field that will see many customers in the near term interested in verifiable quantum-generated random numbers."

As background, CQC was part of the founding group of startups in the IBM Q Network's startup program, announced in 2018. IBM invested in CQC in January of 2020. CQC recently became the first startup-based Hub in the IBM Q Network, working with other members on chemistry, optimization, finance, and quantum machine learning and natural language processing to advance the industry's quantum computing ecosystem.

29 Howard U. to Lead IBM's First Quantum Education, Research Initiative for HBCUs

by WI Web Staff

IBM announced Thursday its first IBM Quantum education and research initiative for historically Black colleges and universities.

The initiative, aimed at driving a diverse and inclusive quantum workforce, will be led by Howard University and 12 additional HBCUs, with the IBM-HBCU Quantum Center offering access to its quantum computers, as well as collaboration on academic, education, and community outreach programs, according to a Howard press statement.

“We believe that in order to expand opportunity for diverse populations, we need a diverse talent pipeline of the next generation of tech leaders from HBCUs,” Carla Grant Pickens, IBM chief global diversity and inclusion officer, said in the statement. “Diversity and inclusion is what fuels innovation and students from HBCUs will play a significant part of what will drive innovations for the future like quantum computing, cloud and artificial intelligence.”

Also, as part of the company's continued efforts to prepare and develop talent at HBCUs from all STEM disciplines, IBM will make a multi-year $100M investment in technology, assets, resources and skills development through partnerships with additional HBCUs through the IBM Skills Academy Academic Initiative.

The 13 HBCUs intending to participate in the Quantum Center were prioritized based on their research and education focus in physics, engineering, mathematics, computer science, and other STEM fields. They include: Albany State University, Clark Atlanta University, Coppin State University, Hampton University, Howard University, Morehouse College, Morgan State University, North Carolina A&T, Southern University, Texas Southern University, University of the Virgin Islands, Virginia Union University, and Xavier University of Louisiana.

“Howard University has prioritized our efforts to support our students' pathway to STEM fields for many years with exciting results as we witness more and more graduates becoming researchers, scientists and engineers with renown national companies,” said Howard President Wayne A.I. Frederick. “Our faculty and students look forward to collaborating with our peer institutions through the IBM-HBCU Quantum Center. We're excited to share best practices and work together to prepare students to participate in a quantum-ready workforce.”

17 Sep 2020

30 The Phish Scale: NIST-Developed Method Helps IT Staff See Why Users Click on Fraudulent Emails

by NIST

https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click

Researchers at the National Institute of Standards and Technology (NIST) have developed a new method called the Phish Scale that could help organizations better train their employees to avoid a particularly dangerous form of cyberattack known as phishing.

By 2021, global cybercrime damages will cost $6 trillion annually, up from $3 trillion in 2015, according to estimates from the 2020 Official Annual Cybercrime Report by Cybersecurity Ventures.

One of the more prevalent types of cybercrime is phishing, a practice where hackers send emails that appear to be from an acquaintance or trustworthy institution. A phishing email (or phish) can tempt users with a variety of scenarios, from the promise of free gift cards to urgent alerts from upper management. If users click on links in a phishing email, the links can take them to websites that could deposit dangerous malware into the organization's computers.

Many organizations have phishing training programs in which employees receive fake phishing emails generated by the employees' own organization to teach them to be vigilant and to recognize the characteristics of actual phishing emails. Chief information security officers (CISOs), who often oversee these phishing awareness programs, then look at the click rates, or how often users click on the emails, to determine if their phishing training is working. Higher click rates are generally seen as bad because it means users failed to notice the email was a phish, while low click rates are often seen as good.

However, numbers alone don't tell the whole story. "The Phish Scale is intended to help provide a deeper understanding of whether a particular phishing email is harder or easier for a particular target audience to detect," said NIST researcher Michelle Steves. The tool can help explain why click rates are high or low.

The Phish Scale uses a rating system that is based on the message content in a phishing email. This can consist of cues that should tip users off about the legitimacy of the email and the premise of the scenario for the target audience, meaning whichever tactics the email uses would be effective for that audience. These groups can vary widely, including universities, business institutions, hospitals and government agencies.

The new method uses five elements that are rated on a 5-point scale that relate to the scenario's premise. The overall score is then used by the phishing trainer to help analyze their data and rank the phishing exercise as low, medium or high difficulty.

The significance of the Phish Scale is to give CISOs a better understanding of their click-rate data instead of relying on the numbers alone. A low click rate for a particular phishing email can have several causes: The phishing training emails are too easy or do not provide relevant context to the user, or the phishing email is similar to a previous exercise. Data like this can create a false sense of security if click rates are analyzed on their own without understanding the phishing email's difficulty.

By using the Phish Scale to analyze click rates and collecting feedback from users on why they clicked on certain phishing emails, CISOs can better understand their phishing training programs, especially if they are optimized for the intended target audience.

The Phish Scale is the culmination of years of research, and the data used for it comes from an "operational" setting, very much the opposite of a laboratory experiment with controlled variables. "As soon as you put people into a laboratory setting, they know," said Steves. "They're outside of their regular context, their regular work setting, and their regular work responsibilities. That is artificial already. Our data did not come from there."

This type of operational data is both beneficial and in short supply in the research field. "We were very fortunate that we were able to publish that data and contribute to the literature in that way," said NIST researcher Kristen Greene.

As for next steps, Greene and Steves say they need even more data. All of the data used for the Phish Scale came from NIST. The next step is to expand the pool and acquire data from other organizations, including nongovernmental ones, and to make sure the Phish Scale performs as it should over time and in different operational settings. “We know that the phishing threat landscape continues to change,” said Greene. “Does the Phish Scale hold up against all the new phishing attacks? How can we improve it with new data?” NIST researcher Shaneé Dawkins and her colleagues are now working to make those improvements and revisions.

Detailed steps for the DIY tool are listed in the methods section of the paper.

In the meantime, the Phish Scale provides a new way for computer security professionals to better understand their organization’s phishing click rates, and ultimately improve training so their users are better prepared against real phishing scenarios.

31 Miraex joins IBM Q Network to collaborate on distributed quantum computing

https://www.swissquantumhub.com/miraex-joins-ibm-q-network-to-collaborate-on-distributed-quantum-computing/

Swiss-based startup Miraex has joined the IBM Q Network. Using IBM’s state-of-the-art quantum infrastructure and accompanying expertise, Miraex is working on simulation and pulse-level control of quantum hardware.

Miraex has been founded by an international team of entrepreneurs and located at EPFL’s Innovation Park in Lausanne. The team of experienced quantum scientists and engineers develops photonic and quantum full-stack solutions for next-generation sensing, networking and computing. They are supported by several initiatives in Switzerland (VentureKick, ESA BIC, InnoBooster GRS, IMD, . . .) and graduated from Creative Destruction Lab (CDL) in Toronto.

A key focus of the Miraex team’s quantum roadmap is to build the hardware that solves the challenge of connecting different QPUs (quantum processing units) together. This will enable the realization of a quantum internet, i.e. a distributed network of quantum computers connected via secure optical communication channels. Almost a decade of research made Miraex come up with their quantum converter, which can convert stationary (microwave) qubits into flying (optical) qubits and vice versa.

32 Adopting Quantum-Safe Cryptography: Why Y2Q Will Be Too Late

by Philip Lafrance

https://securityboulevard-com.cdn.ampproject.org/c/s/securityboulevard.com/2020/09/adopting-quantum-cryptography-why-y2q-will-be-too-late/amp/

Standards bodies, government organizations and research centers are weighing in on preparing for the threat that quantum computers pose to encryption. The latest from the National Institute of Standards and Technology (NIST): “The race to protect sensitive electronic information against the threat of quantum computers has entered the home stretch.”

The institute has been in the process of evaluating and standardizing quantum-safe algorithms for key establishment and digital signatures. NIST recently selected the final round of post-quantum cryptography candidates and plans to release the initial standard for quantum-resistant cryptography in 2022, saying that Round 3 will last 12 to 18 months. When it comes to migration, that's a blink of an eye!

"Anyone that wants to make sure that their data is protected for longer than 10 years should move to alternate forms of encryption now," warned Arvind Krishna, director of IBM Research, in a ZDNet article.

Quantum computers will be able to break the asymmetric encryption and signature algorithms we currently rely on in our networks and security infrastructure. Most experts project that a large-scale quantum computer capable of breaking our encryption will be built sometime within the next seven to 15 years. Meanwhile, Google and IBM both claim they can build quantum computers as soon as in the next five years, according to The Telegraph.

Organizations that rely on classical cryptography, such as RSA or ECC, will need to migrate their security infrastructure to a quantum-safe state to offer adequate protection in the new technology paradigm. As RSA or ECC-based systems are essentially ubiquitous around the world today, this represents the largest, and most difficult, technology migration in human history.

Governments and organizations around the world, including significant threat actors, are pouring vast amounts of money and resources toward the development of large-scale quantum computers and related quantum technologies.

Taking Action Sooner Rather Than Later

Quantum-safe migration planning can be extremely complex and resource-intensive. Organizations must create and execute plans to protect their networks, infrastructures, digital assets and more from quantum-enabled attacks. This quantum-safe planning involves:

- Understanding where the organization currently uses cryptography.
- Understanding the security dependencies throughout the organization and its supply chains.
- Understanding where and how their systems are vulnerable to quantum-enabled attacks.
- Deciding on exactly how to migrate current systems to next-generation technologies.
- Allocating budgets and receiving leadership approval.
- Executing the migration.

Many organizations, especially government agencies, have taken 10 to 15+ years to complete smaller cryptographic migrations in the past. In comparison, the quantum threat and subsequent migration required is unprecedented in scope and scale.

The European Telecommunications Standards Institute (ETSI) has published multiple reports investigating various aspects of quantum computing, including an analysis of different case studies and deployment scenarios, as well as a general assessment of the quantum threat. Examples of security threats caused by quantum computers include"harvest and decrypt" attacks, whereby encrypted data is captured in transit and stored until the attacker has access to a quantum computer capable of decrypting it.

If encrypted sensitive data is stolen today, it can be "saved" and will be accessible once a sufficiently powerful quantum computer is available. If sensitive data – client information, financial data, healthcare data, trade secrets, classified information – needs to remain confidential for seven years or longer, then it should be considered at-risk, requiring quantum-safe protections today. Harvest and decrypt attacks are an issue for data transmissions that contain information that extends beyond that. This implies that the quantum threat is a highly relevant concern for many of today's secure communications, including TLS or VPN protected sessions.

NIST concurs, noting that once quantum computers are in place,"individuals can record and capture current information and communications and gain access to the raw content once quantum computing technology is available. This includes all recorded communications and stored information protected by those public-key algorithms."

According to a 2020 report by the RAND Corporation,"There is little to no margin of safety for beginning the migration to [post-quantum cryptography] PQC[1]. The vulnerability presented by quantum computers will affect every government body, critical infrastructure, and industry sector." Organizations need to ask themselves what will need to be upgraded and when.

Let's take a look at satellite manufacturers, for example. Satellites take years to develop and are often expected to operate for a long time. A satellite launched into space today without some sort of embedded quantum-safe security will essentially be space junk well before the expected end of its useful life if it cannot be trusted to secure data transmissions. What if the satellite's sensitive communications are compromised by quantum-capable attackers, or if confidentiality requirements are threatened by harvest-and-decrypt attacks?

Similar examples can be seen in the enterprise space. A small organization with limited infrastructure and relatively uncomplicated systems should easily be able to identify where they use cryptography today and form an actionable strategy to ensure it has adequate quantum-safe protections. This includes ensuring that vendors in the organization's supply chain are also adding the necessary quantum-safe protections to their products. Of course, this action plan must also address transitioning the security of internally developed systems to quantum-safe states in a relatively short amount of time.

The same cannot be said for larger enterprises running vast networks, possibly with integrated cloud capabilities and disintegrating network security perimeters – due to parameters such as BYOD policies, increased volume of remote workers, high employee or contractor turnover and so on. Discovering and documenting where cryptography is deployed in large enterprises can take years, even with significant resources invested in the project.

Determining how to upgrade systems to ensure they are protected from quantum-enabled attacks also adds several additional years to the migration plan. Add in the budget considerations, testing requirements, compliance obligations, proof of concept projects and the actual eventual deployment, and suddenly the migration timelines for many organizations extend beyond the expected advent of large-scale quantum computers.

What Are Quantum-Safe Options for Organizations?

There are five different branches of mathematics that are currently believed to yield quantum-safe asymmetric cryptographic algorithms. Most are represented in the current NIST PQC project. These math derivatives are based on lattices, hash functions, supersingular isogenies, coding theory and systems of multivariate quadratic polynomials. Each branch has its own advantages and disadvantages, and the current candidates vary greatly in terms of key and data sizes, power consumption and algorithm runtimes (for key generation or encapsulation, signature generation, signature verification, etc.).

[1] Post-quantum cryptography is often referred to as quantum-safe cryptography

Once NIST publishes initial standards, organizations will have to be careful in selecting algorithms most suited to their own requirements. Importantly, this involves understanding exactly what the needs and requirements of the organization are.

This leaves us with a chasm between today and when standards-compliant implementations can be certified and accredited. We recommend that organizations investigate hybrid (classic and quantum) or crypto-agile solutions. Crypto agility means that cryptographic components of systems or their sub-systems can be easily removed and replaced with minimal disruption to the rest of the system. In terms of executing any sort of cryptographic transition, not just one from classic to quantum-safe cryptography, crypto agility provides an attractive method to substantially reduce technology switching costs.

There is a small margin of error for beginning the quantum-safe migration. If organizations wait until NIST finalizes standards before they start investigating or implementing quantum-safe solutions, they very likely will not have enough time to properly form and execute their migration plan, leaving them susceptible to quantum-enabled attacks. For organizations that require standards before they can deploy new algorithms in their infrastructures or production environments, it is critical that they engage in proof-of-concept planning now to ensure they are ready to roll out the new technologies in a responsible timeline.

Here are the initial migration steps we recommend as organizations transition to a quantum-safe state:

(i) Discover where the organization is using cryptography and catalogue what type of cryptography it is and what information it's protecting. Intuitively, this should be easy enough to do, but in practice, this discovery phase may be prohibitively complex and expensive. Many organizations have given this task little attention to date and don't know where to start. For organizations with large shadow IT departments or poorly documented cryptography, even a large audit might not guarantee complete coverage.

(ii) The discovery and audit process should also investigate the need for quantum-safe protections for partner organizations or vendors in the supply chain. An organization can do everything it can to make itself quantum-safe, but if it is integrating OEM components that are not quantum-safe into their own products or services, then the organization might still be quantum-vulnerable.

(iii) Once an audit is completed, the next steps include determining how to upgrade, transition or migrate vulnerable cryptography to versions certifiable as quantum-safe. Again, this step includes working with partners and suppliers.

The work required to become quantum-safe ready is vast and could take years to accomplish, depending on the organization's network and infrastructure complexity.

Making the relevant inquiries now is essential to minimize the amount of time it will take organizations, partners and suppliers to make this cryptographic shift. Asking partners and suppliers about their road maps and timelines for quantum-safe migrations will be an essential exercise. Without sufficient demand from their customers, OEMs may put off their own quantum-safe migrations.

15 Sep 2020

33 IBM's Roadmap For Scaling Quantum Technology

by Jay Gambetta

https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/

Back in 1969, humans overcame unprecedented technological hurdles to make history: we put two of our own on the Moon and returned them safely. Today's computers are capable, but assuredly earthbound when it comes to accurately capturing the finest details of our universe. Building a device that truly captures the behavior of atoms – and can harness these behaviors to solve some of the most challenging problems of our time – might seem impossible if you limit your thinking to the computational world you know. But like the Moon landing, we have an ultimate objective to access a realm beyond what's possible on classical computers: we want to build a large-scale quantum computer. The future's quantum computer will pick up the slack where classical computers falter, controlling the behavior of atoms in order to run revolutionary applications across industries, generating world-changing materials or transforming the way we do business.

Today, we are releasing the roadmap that we think will take us from the noisy, small-scale devices of today to the million-plus qubit devices of the future. Our team is developing a suite of scalable, increasingly larger and better processors, with a 1000-plus qubit device, called **IBM Quantum Condor**, targeted for the end of 2023. In order to house even more massive devices beyond Condor, we're developing a dilution refrigerator larger than any currently available commercially. This roadmap puts us on a course toward the future's million-plus qubit processors thanks to industry-leading knowledge, multidisciplinary teams, and agile methodology improving every element of these systems. All the while, our hardware roadmap sits at the heart of a larger mission: to design a full-stack quantum computer deployed via the cloud that anyone around the world can program.

The IBM Quantum team builds quantum processors – computer processors that rely on the mathematics of elementary particles in order to expand our computational capabilities, running quantum circuits rather than the logic circuits of digital computers. We represent data using the electronic quantum states of artificial atoms known as superconducting transmon qubits, which are connected and manipulated by sequences of microwave pulses in order to run these circuits. But qubits quickly forget their quantum states due to interaction with the outside world. The biggest challenge facing our team today is figuring out how to control large systems of these qubits for long enough, and with few enough errors, to run the complex quantum circuits required by future quantum applications.

IBM has been exploring superconducting qubits since the mid-2000s, increasing coherence times and decreasing errors to enable multi-qubit devices in the early 2010s. Continued refinements and advances at every level of the system from the qubits to the compiler allowed us to put the first quantum computer in the cloud in 2016. We are proud of our work. Today, we maintain more than two dozen stable systems on the IBM Cloud for our clients and the general public to experiment on, including our 5-qubit IBM Quantum Canary processors and our 27-qubit IBM Quantum Falcon processors – on one of which we recently ran a long enough quantum circuit to declare a Quantum Volume of 64. This achievement wasn't a matter of building more qubits; instead, we incorporated improvements to the compiler, refined the calibration of the two-qubit gates, and issued upgrades to the noise handling and readout based on tweaks to the microwave pulses. Underlying all of that is hardware with world-leading device metrics fabricated with unique processes to allow for reliable yield.

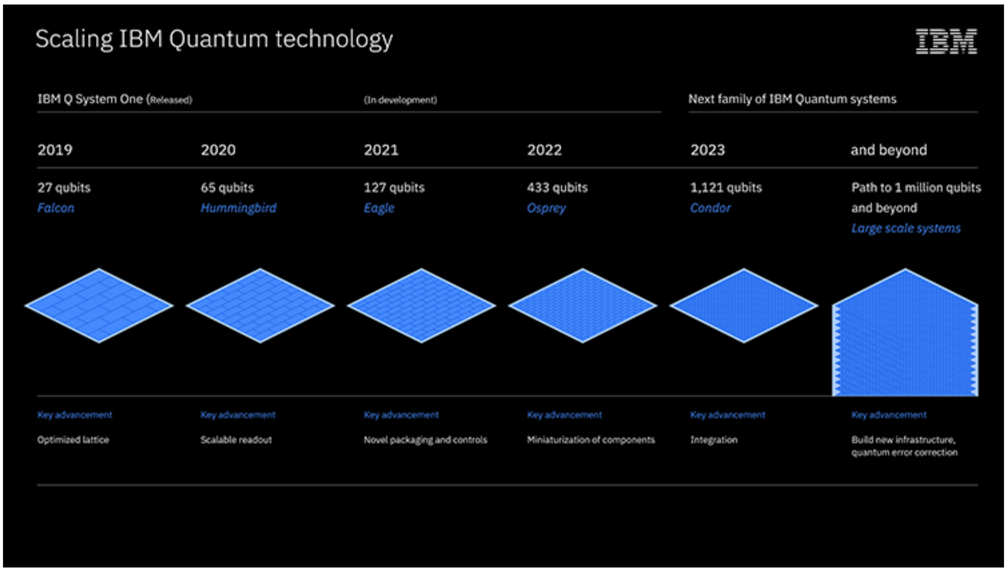
Simultaneous to our efforts to improve our smaller devices, we are also incorporating the many lessons learned into an aggressive roadmap for scaling to larger systems. In fact, this month we quietly released our 65-qubit IBM Quantum Hummingbird processor to our IBM Q Network members. This device features 8:1 readout multiplexing, meaning we combine readout signals from eight qubits into one, reducing the total amount of wiring and components required for readout and improving our ability to scale, while preserving all of the high performance features from the Falcon generation of processors. We have significantly reduced the signal processing latency time in the associated control system in preparation for upcoming feedback and feed-forward system capabilities, where we'll be able to control qubits based on classical conditions while the quantum circuit runs.

Next year, we'll debut our 127-qubit IBM Quantum Eagle processor. Eagle features several upgrades in order to surpass the 100-qubit milestone: crucially, through-silicon vias (TSVs) and multi-level wiring provide the ability to effectively fan-out a large density of classical control signals while protecting the qubits in a separated layer in order to maintain high coherence times. Meanwhile, we've struck a delicate balance of connectivity and reduction of crosstalk error with our fixed-frequency approach to two-qubit gates and hexagonal qubit arrangement introduced by Falcon. This qubit layout will allow us to implement the "heavy-hexagonal" error-correcting code that our team debuted last year, so as we scale up the number of physical qubits, we will also be able to explore how they'll work together as error-corrected logical qubits – every processor we design has fault tolerance considerations taken into account.

With the Eagle processor, we will also introduce concurrent real-time classical compute capabilities that will allow for execution of a broader family of quantum circuits and codes.

The design principles established for our smaller processors will set us on a course to release a 433-qubit IBM Quantum Osprey system in 2022. More efficient and denser controls and cryogenic infrastructure will ensure that scaling up our processors doesn't sacrifice the performance of our individual qubits, introduce further sources of noise, or take up too large a footprint.

In 2023, we will debut the 1121-qubit IBM Quantum Condor processor, incorporating the lessons learned from previous processors while continuing to lower the critical two-qubit errors so that we can run longer quantum circuits. We think of Condor as an inflection point, a milestone that marks our ability to implement error correction and scale up our devices, while simultaneously complex enough to explore potential Quantum Advantages – problems that we can solve more efficiently on a quantum computer than on the world's best supercomputers.



Scaling IBM Quantum technology

IBM Q System One (Released)		(In development)		Next family of IBM Quantum systems	
2019	2020	2021	2022	2023	and beyond
27 qubits *Falcon*	65 qubits *Hummingbird*	127 qubits *Eagle*	433 qubits *Osprey*	1,121 qubits *Condor*	Path to 1 million qubits and beyond *Large scale systems*
Key advancement Optimized lattice	Key advancement Scalable readout	Key advancement Novel packaging and controls	Key advancement Miniaturization of components	Key advancement Integration	Key advancement Build new infrastructure, quantum error correction

The development required to build Condor will have solved some of the most pressing challenges in the way of scaling up a quantum computer. However, as we explore realms even further beyond the thousand qubit mark, today's commercial dilution refrigerators will no longer be capable of effectively cooling and isolating such potentially large, complex devices.

That's why we're also introducing a 10-foot-tall and 6-foot-wide "super-fridge", internally codenamed "Goldeneye", a dilution refrigerator larger than any commercially available today. Our team has designed this behemoth with a million-qubit system in mind – and has already begun fundamental feasibility tests. Ultimately, we envision a future where quantum interconnects link dilution refrigerators each holding a million qubits like the intranet links supercomputing processors, creating a massively parallel quantum computer capable of changing the world.

Knowing the way forward doesn't remove the obstacles; we face some of the biggest challenges in the history of technological progress. But, with our clear vision, a fault-tolerant quantum computer now feels like an achievable goal within the coming decade.

13 Sep 2020

34 Spin-Based Quantum Computing Breakthrough: Physicists Achieve Tunable Spin Wave Excitation

by MOSCOW INSTITUTE OF PHYSICS AND TECHNOLOGY

https://scitechdaily.com/spin-based-quantum-computing-breakthrough-physicists-achieve-tunable-spin-wave-excitation/

Physicists from MIPT and the Russian Quantum Center, joined by colleagues from Saratov State University and Michigan Technological University, have demonstrated new methods for controlling spin waves in nanostructured bismuth iron garnet films via short laser pulses. Presented in Nano Letters, the solution has potential for applications in energy-efficient information transfer and spin-based quantum computing.

A particle's spin is its intrinsic angular momentum, which always has a direction. In magnetized materials, the spins all point in one direction. A local disruption of this magnetic order is accompanied by the propagation of spin waves, whose quanta are known as magnons.

Unlike the electrical current, spin wave propagation does not involve a transfer of matter. As a result, using magnons rather than electrons to transmit information leads to much smaller thermal losses. Data can be encoded in the phase or amplitude of a spin wave and processed via wave interference or nonlinear effects.

Simple logical components based on magnons are already available as sample devices. However, one of the challenges of implementing this new technology is the need to control certain spin wave parameters. In many regards, exciting magnons optically is more convenient than by other means, with one of the advantages presented in the recent paper in Nano Letters.

The researchers excited spin waves in a nanostructured bismuth iron garnet. Even without nanopatterning, that material has unique optomagnetic properties. It is characterized by low magnetic attenuation, allowing magnons to propagate over large distances even at room temperature. It is also highly optically transparent in the near infrared range and has a high Verdet constant.

The film used in the study had an elaborate structure: a smooth lower layer with a one-dimensional grating formed on top, with a 450-nanometer period. This geometry enables the excitation of magnons with a very specific spin distribution, which is not possible for an unmodified film.

To excite magnetization precession, the team used linearly polarized pump laser pulses, whose characteristics affected spin dynamics and the type of spin waves generated. Importantly, wave excitation resulted from optomagnetic rather than thermal effects.

The researchers relied on 250-femtosecond probe pulses to track the state of the sample and extract spin wave characteristics. A probe pulse can be directed to any point on the sample with a desired delay relative to the pump pulse. This yields information about the magnetization dynamics in a given point, which can be processed to determine the spin wave's spectral frequency, type, and other parameters.

Unlike the previously available methods, the new approach enables controlling the generated wave by varying several parameters of the laser pulse that excites it. In addition to that, the geometry of the nanostructured film allows the excitation center to be localized in a spot about 10 nanometers in size. The nanopattern also makes it possible to generate multiple distinct types of spin waves. The angle of incidence, the wavelength and polarization of the laser pulses enable the resonant excitation of the waveguide modes of the sample, which are determined by the nanostructure characteristics, so the type of spin waves excited can be controlled. It is possible for each of the characteristics associated with optical excitation to be varied independently to produce the desired effect.

"Nanophotonics opens up new possibilities in the area of ultrafast magnetism," said the study's co-author, Alexander Chernov, who heads the Magnetic Heterostructures and Spintronics Lab at MIPT. "The creation of practical applications will depend on being able to go beyond the submicrometer scale, increasing operation speed and the capacity for multitasking. We have shown a way to overcome these limitations by nanostructuring a magnetic material. We have successfully localized light in a spot few tens of nanometers across and effectively excited standing spin waves of various orders. This type of spin waves enables the devices operating at high frequencies, up to the terahertz range."

The paper experimentally demonstrates an improved launch efficiency and ability to control spin dynamics under optical excitation by short laser pulses in a specially designed nanopatterned film of bismuth iron garnet. It opens up new prospects for magnetic data processing and quantum computing based on coherent spin oscillations.

12 Sep 2020

35 Don't pay the ransom, mate. Don't even fix a price, say Australia's cyber security bods

by Gareth Corfield

https://www.theregister.com/2020/09/12/follow_security_basics_and_you/

Most online attacks could be easily avoided by following basic cyber security advice, Australia's national cyber security bureau has said – even as it warned that the impact and severity of things like ransomware attacks are getting worse and worse.

"Cybercriminals follow the money," said the Australian Cyber Security Centre (ACSC) in its annual report for 2019-20, published earlier this week.

"Over the past 12 months the ACSC has observed real-world impacts of ransomware incidents, which have typically originated from a user executing a file received as part of a spearphishing campaign," said the agency, adding that after the initial breach attackers typically try to exploit remote desktop-type apps to hunt for anything worth stealing – or deleting.

ACSC was busiest in April 2020, when it had 318 “cyber security incidents” reported to it.

Out of 2266 incidents that the agency responded to over the 12-month period, 803 were targeted against Australia’s federal or state level governments – though the ACSC put this down to the public sector’s willingness to report incidents to it, as distinct from the private sector.

Most attacks can easily be mitigated, said ACSC, through “measures such as not responding to unsolicited emails and text messages, implementing multi-factor authentication and never providing another party with remote access to your computer.”

Those attacks include June’s cyber-assaults against the Lion brewery, which were remarkably closely timed as China stepped up diplomatic pressure on Australia over international cooperation.

“Many of these [attacks] could have been avoided or substantially mitigated by good cyber security practices,” sighed the ACSC in the report, which covered the months July 2019-June 2020.

The infoseccers strongly advised against paying the criminals:

> Paying a ransom does not guarantee decryption of data. Open source reporting indicates several instances where an entity paid the ransom but the keys to decrypt the data were not provided. The ACSC has also seen cases where the ransom was paid, the decryption keys were provided, but the adversary came back a few months later and deployed ransomware again. The likelihood that an Australian organisations will be retargeted increases with every successful ransom payment. . . .
>
> It is generally much easier and safer to restore data from a backup than attempting to decrypt ransomware affected data.

While it won’t surprise regular Register readers to hear that ransomware is “one of the most significant threats” to online businesses in Aus (and beyond), the ACSC is already looking ahead at towards how 5G and increased digital connectivity across their nation will expose more and more people and businesses to the risks of being online.

5G networks and Internet of Things devices “require new thinking about how best to adopt them securely,” opined ACSC. Britain has published design standards for IoT devices, while on 5G the US has addressed potential vendor security problems by shutting out those they deem to be problematic vendors.

11 Sep 2020

36 China claims quantum leap with machine declared a million times greater than Google’s Sycamore

by Stephen Chen

https://www.scmp.com/news/china/science/article/3101219/china-claims-quantum-leap-machine-declared-million-times-greater

A Chinese physicist claimed to have built a quantum computer that would leave Western competitors in the dust, but he and his team said they needed to “further verify” the claim.

Pan Jianwei, a physicist from the University of Science and Technology of China, announced at a lecture at Westlake University, Hangzhou, on September 5 that a new machine had recently achieved “quantum supremacy” one million times greater than the record currently held by Sycamore, a quantum computer built by Google.

Sycamore completed in about 200 seconds a calculation that would keep the fastest computer on Earth busy for 10,000 years, according to a paper published by Google researchers last year.

Pan’s claim was reported by Anhui Daily and other media on the mainland.

Pan’s team issued a statement on Weibo on Tuesday that they were “deeply worried” by these reports because Pan had been quoted out of context.

The results were still preliminary, and there was “no 100% guarantee until further verification,” Pan was quoted as saying in the statement.

By the time of publishing this South China Morning Post report, Pan’s team had not released a paper to provide more details about their work.

A quantum computer uses qubits, or subatomic particles in various quantum states to perform many calculations at the same time. Some scientists believe the technology could one day be used to hack into a bank account protected by a password, among other applications.

A general purpose quantum computer could still be decades away, however. Most existing machines perform only very specific tasks and have nothing to do with code breaking.

Pan’s quantum computer, for instance, simulates how light bounces through a chamber filled with crystals. When a particle of light hits a crystal, it goes either left or right and hits another crystal, and then another. As the number of light particles increases, the situation becomes extremely complicated. Simulating this process could strain the resources of the most powerful computer, but would be much easier on a quantum computer.

When Pan’s team started building a device to perform this particular task, known as boson sampling, it could handle 10 qubits. Now they have achieved 50 qubits, according to Pan.

Google’s Sycamore handles 53 qubits but was built with a different design, known as “random circuit”, to deal with a different task. Neither Pan nor his team explained how they compared the performance of the two machines.

Both were built to demonstrate “quantum supremacy”, or the idea that quantum computers could do better than their conventional counterparts, at least on some specific tasks.

But the idea was not without controversy. IBM, for instance, alleged that Google had exaggerated their claim by using an outdated algorithm that stretched the runtime on supercomputers from two days to over 10,000 years.

Pan led the development of the world’s first quantum satellite and the construction of the longest quantum communication network from Beijing to Shanghai which, in theory, could not be tapped into. His team has received generous and consistent financial support from the Chinese government for nearly two decades to bring China‘s quantum technology to a world-leading position.

A scientist in his team said they were under pressure to prove the worth of the government’s investments.

“Not all fundamental research work has an immediate application in sight,” said the physicist who asked not to be named because of the sensitivity of the issue.

A major challenge for quantum computing is that it usually needs to work in extremely cold and isolated environments. Subatomic particles are fragile, short-lived and prone to error with even slight disturbance from the surroundings.

37 Quantum computers threaten to end digital security. Here's what's being done about it

by JEREMY KAHN

https://fortune.com/2020/09/11/post-quantum-encryption-algorithm-nist/

For much of the past decade, cybersecurity experts have been warning of a looming threat: the advent of quantum computers.

These machines, which use principles of quantum physics to represent information, will one day be powerful enough to crack the most widely used encryption systems, rendering almost all digital communication insecure.

The question has always been exactly when that day would arrive. The most common digital encryption technique, RSA, which was invented in 1977, is based on multiplying two large prime numbers. One way to break it is to figure out what those two large primes were. In 1994, mathematician Peter Shor invented an algorithm, that if run on a sufficiently powerful quantum computer, would easily find these two primes. But at the time, quantum computers were still purely theoretical machines.

The first working quantum computers were built over a decade ago. But most were either not designed in a way that would allow them to run Shor's algorithm. Others were simply not powerful enough to do so for a very large prime multiple. The moment when cybersecurity experts would have to worry about quantum computer-equipped hackers seemed a long way off – at least a quarter century by some estimates – and there were far more pressing threats.

But not anymore. Last year, Google claimed it had achieved a milestone known as "quantum supremacy," having built a quantum computer capable of performing a calculation that could not be done on a traditional computer in a reasonable length of time.

Google's machine is still unable to break RSA. But the rapid progress in building quantum hardware along with some clever advancements in algorithms mean the timeline for Shor's algorithm rendering RSA obsolete have been moved up considerably. If lucky, we may have more than decade of data privacy protection left, experts say. But some think we have at best five years – maybe less.

In 2016, the U.S. National Security Agency issued a stark warning that government agencies and companies "must act now" to begin moving to a new encryption standard that is safe from quantum computer-based attacks. The only problem? No one was sure exactly what that encryption standard should be.

That's why the National Institute of Standards and Technology (NIST), an agency with the U.S. Department of Commerce that is responsible for recommending standards that are often adopted by both government and business, began a competition almost three years ago to select new encryption techniques that would be resistant to attacks from quantum computers.

These new "post-quantum" encryption and digital signature methods will likely become mandatory for all U.S. government departments and for many companies that do business with the government, especially in defense and intelligence. Because of the size of the U.S. market, they are also likely to become the new global security standard. NIST is now on the verge of picking the winning encryption algorithms – and ushering in a new era in cybersecurity.

In July, the standards agency announced that it had winnowed an initial group of 82 candidates down to a long-list of 15, including four main finalists for encryption and three for digital signatures, which use cryptography to verify whether electronic messages and documents are authentic. (Eight alternates will advance to the final round as well.) NIST has said it will announce its final endorsements for a new encryption standard within the next 18 months.

So what does the NIST long-list tell us about the future of cybersecurity? Well, there's a good chance that it will involve something called lattice-based cryptography. Three of the four encryption finalists come from this family of algorithms.

Lattice-based cryptography is based on the unique mathematical properties of grids of evenly-spaced points, or lattices. Because the points are evenly spaced, it turns out that from just two coordinates of the grid it is possible to compute all the points within the same lattice. But figuring out whether any given point is in the lattice can be difficult if the lattice is in many thousands of dimensions and if the angles between points in the grid are far from perpendicular. A number of encryption schemes have been created that use these properties to create a public key and a private key that work together – because they are calculated from the same lattice – but in which it is extremely difficult to derive the private key from the public key alone.

But some cybersecurity experts are surprised that NIST has leaned so heavily towards this kind of post-quantum encryption. That's because while lattice-based problems are mathematically difficult and, unlike RSA, are not susceptible to Shor's algorithm, they have not been mathematically proven to be impervious to a quantum computer-based attack. "We say that quantum algorithms cannot break them yet," Delaram Kahrobaei, a professor of cybersecurity at the University of York, in England, says. "But tomorrow someone comes up with another quantum algorithm that might break them."

Kahrobaei says she is disappointed to see that candidates from other families of potential post-quantum algorithms did not make it onto the final list. This includes multivariate cryptography, which is based on the difficulty of solving systems of complex quadratic equations (remember those from high school algebra?), and group-based cryptography, which is the area that Kahrobaei herself works on. It is based on yet another area of mathematics involving transforming a set of numbers by combining elements, often according to elaborate geometric patterns, such as braids.

The only non-lattice post-quantum encryption candidate among the NIST finalists comes from a cryptographic family known as code-based algorithms. These all involve adding some sort of error to data – like a classic code where you shift the alphabet over two letters so that A is encoded as C and B as D, and so on. This error is then corrected to decrypt the message. The post-quantum algorithm NIST has chosen is called Classic McEliece, named for an error-correcting code algorithm invented by mathematician Robert McEliece in the late 1970s. It applies a different random error to each piece of information that's encoded – which in theory makes it impossible to break without knowing the key.

"McEliece's system has been around for 41 years and been attacked by the crypto community for all that time without finding a vulnerability," Andersen Cheng, the co-founder and chief executive officer of Post-Quantum Group, a London-based cybersecurity company that joined forces with another team, led by Daniel Bernstein, a noted cryptographer at the University of Illinois in Chicago, to work on the Classic McEliece submission that made it to the long list of NIST finalists.

In 2019, the German Federal Office for Information Security (BSI), concerned that the NIST process was taking too long, recommended the Classic McEliece as one of its two recommended post-quantum encryption standards. (The other was a lattice-based method that is among NIST's alternate candidates.) Cheng says he suspects that NIST, like the German government, will ultimately endorse two standards – Classic McEliece and one of the lattice methods.

The only drawback of the McEliece algorithm, Cheng says, is that the relatively lengthy keys the method uses, and the computational complexity of the algorithm, means it takes more time for a computer to encrypt and decrypt information than with its lattice-based competitors. "It's slower by a few milliseconds," Cheng says. But he says that for exchanging public encryption keys – which is mostly what the algorithm would be used for – the method is still actually faster than RSA.

While there are researchers from established tech companies, such as IBM, Intel, and the chipmaker ARM, involved in the race to find quantum-secure encryption algorithms, what's notable is how relatively few established cybersecurity firms are contenders in the NIST contest. Post-Quantum is among several startups that entered the competition – and which are poised to profit from the move to a new generation of encryption.

Kahrobaei says she expects a host of new companies to spring up to help commercialize post-quantum encryption, just as RSA Security – the company that was founded in 1982 to commercialize the RSA algorithm – became a dominant player in the cybersecurity space for the past three decades.

Cheng says that Post-Quantum Group, which was founded in 2009, once struggled to get chief information security officers and chief information officers at major banks and corporations to take the threat of quantum computers seriously. But, he says, the NIST process has belatedly focused their attention. "Now they know they have to do something in 18 months-time and they are starting to ask questions, 'what can they do?'" he says.

10 Sep 2020

38 New Protocol Corrects Errors Due to Qubit Loss – May Be Key to Development of Large-Scale Quantum Computers

by UNIVERSITÀ DI BOLOGNA

https://scitechdaily.com/new-protocol-corrects-errors-due-to-qubit-loss-may-be-key-to-development-of-large-scale-quantum-computers/

Even quantum computers make mistakes. Their computing ability is extraordinary; indeed, it exceeds that of classical computers by far. This is because circuits in quantum computers are based on qubits that can represent not only 0s or 1s, but also superpositions of 0 and 1 states by using the principles of quantum mechanics. Despite their great potential, qubits are extremely fragile and prone to errors due to the interactions with the external environment.

To solve this crucial issue, an international research group developed and implemented a new protocol that allows for the protection and the correction of the fragile quantum information in case of errors due to qubit loss. This research group published the results of their study in Nature.

"Developing a fully functioning quantum processor still represents a great challenge for scientists across the world," explains Davide Vodola who is one of the authors of the study as well as a researcher at the University of Bologna. "This research allowed us, for the first time, to implement a protocol that can detect and, at the same time, correct errors due to qubit loss. This ability could prove to be essential for the future development of large-scale quantum computers."

We know that quantum processors show a certain tolerance against computational errors. But we know too little about how to prevent and correct the errors that are due to a complete or partial loss of qubits.

When quantum computers elaborate the data, some qubits can be completely lost from the quantum registers or they can transition to unwanted electronic states. The outcome of both these processes is a loss that may render the quantum processor useless. For this reason, devising theory-based and experimental techniques that can analyse and mitigate the consequences of these errors is extremely important.

"To solve this problem, the first thing our research group did was to develop an effective theoretical approach to the issue," says Vodola. "We managed to show that the information stored in a register with some qubits can be protected and fully retrieved in case one of these qubits gets lost."

Then, the research group implemented this protocol in a real-life quantum processor. This is not easy at all, however. Indeed, for assessing whether a qubit is lost, a direct measurement of it will destroy all the information that is contained in the quantum register.

The research group came up with the solution of using an additional qubit that functions as a probe and can assess the presence or absence of other qubits without altering the computing process. This idea worked, allowing the researchers to successfully test their protocol in real-time.

"We are happy with the results of this test on the trapped-ion quantum processor of the University of Innsbruck," confirms Vodola. "The same protocol can be implemented in different quantum computer architectures that are currently under development by other research centers or private institutions."

09 Sep 2020

39 Raccoon attack allows hackers to break TLS encryption 'under certain conditions'

by Catalin Cimpanu

https://www.zdnet.com/article/raccoon-attack-allows-hackers-to-break-tls-encryption-under-certain-conditions/

A team of academics has disclosed today a theoretical attack on the TLS cryptographic protocol that can be used to decrypt the HTTPS connection between users and servers and read sensitive communications.

Named Raccoon, the attack has been described as "really hard to exploit" and its underlying conditions as "rare."

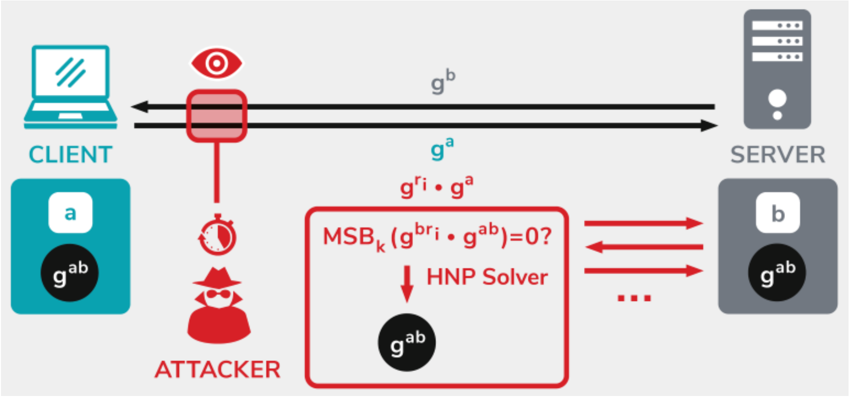
How the Raccoon attack works

According to a paper published today, the Raccoon attack is, at its base, a timing attack, where a malicious third-party measures the time needed to perform known cryptographic operations in order to determine parts of the algorithm.

In the case of a Raccoon attack, the target is the Diffie-Hellman key exchange process, with the aim being to recover several bytes of information.

"In the end, this helps the attacker to construct a set of equations and use a solver for the Hidden Number Problem (HNP) to compute the original premaster secret established between the client and the server," the research team explained.

According to the researchers, all servers that use the Diffie-Hellman key exchange in setting up TLS connections are vulnerable to attacks.



This is a server-side attack and cannot be performed on a client, such as browsers. The attack also needs to be executed for each client-server connection in part, and cannot be used to recover the server's private key and decrypt all connections at once.

Servers that use the Diffie-Hellman key exchange and TLS 1.2 and below are considered vulnerable. DTLS is also impacted.

TLS 1.3 is considered safe.

Not a practical attack

But despite having the capability to decrypt TLS sessions and read sensitive communications, the research team was also the first to admit that the Raccoon attack was also extremely hard to pull off.

For starters, the attack requires that certain and extremely rare conditions be met.

“The vulnerability is really hard to exploit and relies on very precise timing measurements and on a specific server configuration to be exploitable,” researchers said.

“[The attacker] needs to be close to the target server to perform high precision timing measurements. He needs the victim connection to use DH(E) and the server to reuse ephemeral keys. And finally, the attacker needs to observe the original connection.

“For a real attacker, this is a lot to ask for,” academics said.

“However, in comparison to what an attacker would need to do to break modern cryptographic primitives like AES, the attack does not look complex anymore.

“But still, a real-world attacker will probably use other attack vectors that are simpler and more reliable than this attack,” researchers added.

While the attack has been deemed hard to exploit, some vendors have done their due diligence and released patches. Microsoft (CVE-2020-1596), Mozilla, OpenSSL (CVE-2020-1968), and F5 Networks (CVE-2020-5929) have released security updates to block Raccoon attacks.

08 Sep 2020

40 Multi-user communication network paves the way towards the quantum internet

by Tim Wogan

https://physicsworld.com/a/multi-user-communication-network-paves-the-way-towards-the-quantum-internet/

The concept of quantum communication, with security guaranteed by the laws of physics, took the world by storm when first unveiled in 1984. The traditional protocol, however, allows only two people to communicate securely. Attempts to extend this to "quantum networking" have usually proved either insecure or impractically complex. Now, however, researchers in the UK and Austria have demonstrated secure information exchange between eight users spaced all around a city.

The canonical quantum communication protocol relies on two parties generating a secure key by exchanging polarized photons. The security of the link is guaranteed by the fact a third party cannot make a measurement of their state without disturbing them and being detected. Though remarkable, this approach is fundamentally limited to pairwise communication: it does not provide a blueprint for the multi-dimensional quantum network, or "quantum internet" that some researchers have dreamed of, in which multiple users connected together can all communicate simultaneously and securely with any other member of the network.

One obvious way to extend the scheme beyond two people is for the second person to simply act as a link in the chain, repeating the procedure and communicating securely with a third person, who in turn passes the message on until the message reaches its ultimate destination. Quantum networking schemes based on such "trusted nodes" have been developed. The security of such schemes is no longer absolute, however, because a trusted node may not be totally secure. Schemes that avoid trusted nodes have generally proved unfeasibly complex and hardware-intensive or have suffered other problems, such as restricting which users can communicate at any one time.

In 2018, researchers at the Institute for Quantum Optics and Quantum Information in Vienna led by Rupert Ursin demonstrated a scheme in which four users received pairs of entangled photons from a single, laser-pumped crystal source. "I generate these two-by-two, but I generate several such two-by-two pairs in a tiny amount of time," explains project leader Siddarth Koduru Joshi.

This constant stream of entangled photon pairs from a single, central source allowed each of the four parties to become pairwise entangled with each of the other three parties. "If I'm talking to you, I look at stream one, if I'm talking to somebody else, I look at stream two, and so on," says Joshi, now at the University of Bristol. The researchers believed that this scheme provided a simpler, more scalable architecture for secure, trusted-node free information exchange between multiple parties.

In the new work, researchers at the University of Bristol, in collaboration with the Austrian scientists, have confirmed that the technique works, demonstrating simultaneous and secure exchange of information between eight users spaced up to 12.6 km away from the central source around the city of Bristol. "This time, we actually demonstrated quantum communication, and we did this through deployed fibres across the city to show compatibility with existing infrastructure," says Joshi.

Moreover, the researchers added additional multiplexing to simplify the hardware required by each user and make the protocol even more scalable: whereas their original protocol would have required 56 wavelength channels to fully interconnect eight users, their improved version required only 16. The researchers believe their network is the largest trusted-node free quantum network to date.

Quantum and computer engineer Wolfgang Tittel of QuTech at Delft University of Technology in the Netherlands describes the paper as “nice and important work” and is especially impressed by the absence of trusted nodes. An important next step, he says, is the scheme’s integration with quantum repeater technology, which to mitigates photon loss and decoherence and allows entanglement distribution over long distances. This, he says, could “extend the network beyond metropolitan size”.

41 Popular Android apps are rife with cryptographic vulnerabilities

by Zeljka Zorz

https://www.helpnetsecurity.com/2020/09/08/android-apps-cryptographic-vulnerabilities/

Columbia University researchers have released Crylogger, an open source dynamic analysis tool that shows which Android apps feature cryptographic vulnerabilities.

They also used it to test 1780 popular Android apps from the Google Play Store, and the results were abysmal:

- All apps break at least one of the 26 crypto rules
- 1775 apps use an unsafe pseudorandom number generator (PRNG)
- 1764 apps use a broken hash function (SHA1, MD2, MD5, etc.)
- 1076 apps use the CBC operation mode (which is vulnerable to padding oracle attacks in client-server scenarios)
- 820 apps use a static symmetric encryption key (hardcoded)

About Crylogger

Each of the tested apps with an instrumented crypto library were run in Crylogger, which logs the parameters that are passed to the crypto APIs during the execution and then checks their legitimacy offline by using a list of crypto rules.

“Cryptographic (crypto) algorithms are the essential ingredients of all secure systems: crypto hash functions and encryption algorithms, for example, can guarantee properties such as integrity and confidentiality,” the researchers explained.

“A crypto misuse is an invocation to a crypto API that does not respect common security guidelines, such as those suggested by cryptographers or organizations like NIST and IETF.”

To confirm that the cryptographic vulnerabilities flagged by Crylogger can actually be exploited, the researchers manually reverse-engineered 28 of the tested apps and found that 14 of them are vulnerable to attacks (even though some issues may be considered out-of-scope by developers because they require privilege escalation for effective exploitation).

Recommended use

Comparing the results of Crylogger (a dynamic analysis tool) with those of CryptoGuard (an open source static analysis tool for detecting crypto misuses in Java-based applications) when testing 150 apps, the researchers found that the former flags some issues that the latter misses, and vice versa.

The best thing for developers would be to test their applications with both before they offer them for download, the researchers noted. Also, Crylogger can be used to check apps submitted to app stores.

“Using a dynamic tool on a large number of apps is hard, but Crylogger can refine the misuses identified with static analysis because, typically, many of them are false positives that cannot be discarded manually on such a large number of apps,” they concluded.

Worrying findings

As noted at the beginning of this piece, too many apps break too many cryptographic rules. What’s more, too many app and library developers are choosing to effectively ignore these problems.

The researchers emailed 306 developers of Android apps that violate 9 or more of the crypto rules: only 18 developers answered back, and only 8 of them continued to communicate after that first email and provided useful feedback on their findings. They also contacted 6 developers of popular Android libraries and received answers from 2 of them.

The researchers chose not to reveal the names of the vulnerable apps and libraries because they fear that information would benefit attackers, but they shared enough to show that these issues affect all types of apps: from media streaming and newspaper apps, to file and password managers, authentication apps, messaging apps, and so on.

42 Use cases for AI and ML in cyber security

by Aaron Hurst

https://www.information-age.com/use-cases-for-ai-ml-cyber-security-123491392/

As cyber attacks get more diverse in nature and targets, it’s essential that cyber security staff have the right visibility to determine how to solve vulnerabilities accordingly, and AI can help to come up with problems that its human colleagues can’t alone.

“Cyber security resembles a game of chess,” said Greg Day, chief security officer EMEA at Palo Alto Networks. “The adversary looks to outmanoeuvre the victim, the victim aims to stop and block the adversary’s attack. Data is the king and the ultimate prize.

“In 1996, an AI chess system, Deep Blue, won its first game against world champion, Garry Kasparov. It’s become clear that AI can both programmatically think broader, faster and further outside the norms, and that’s true of many of its applications in cyber security now too.”

With this in mind, we explore particular use cases for AI in cyber security that are in place today.

Working alongside staff

Day went on to expand on how AI can work alongside cyber security staff in order to keep the organisation secure.

“We all know there aren’t enough cyber security staff in the market, so AI can help to fill the gap,” he said. “Machine learning, a form of AI, can read the input from SoC analysts and transpose it into a database, which becomes ever expanding.

“The next time the SoC analyst enters similar symptoms they are presented with previous similar cases along with the solutions, based on both statistical analysis and the use of neural nets – reducing the human effort.

“If there’s no previous case, the AI can analyse the characteristics of the incident and suggest which SoC engineers would be the strongest team to solve the problem based on past experiences.

“All of this is effectively a bot, an automated process that combines human knowledge with digital learning to give a more effective hybrid solution.”

Battling bots

Mark Greenwood, head of data science at Netacea, delved into the benefits of bots within cyber security, keeping in mind that companies must distinguish good from bad.

“Today, bots make up the majority of all internet traffic,” explained Greenwood. “And most of them are dangerous. From account takeovers using stolen credentials to fake account creation and fraud, they pose a real cyber security threat.

“But businesses can’t fight automated threats with human responses alone. They must employ AI and machine learning if they’re serious about tackling the ‘bot problem’. Why? Because to truly differentiate between good bots (such as search engine scrapers), bad bots and humans, businesses must use AI and machine learning to build a comprehensive understanding of their website traffic.

“It’s necessary to ingest and analyse a vast amount of data and AI makes that possible, while taking a machine learning approach allows cyber security teams to adapt their technology to a constantly shifting landscape.

“By looking at behavioural patterns, businesses will get answers to the questions ‘what does an average user journey look like’ and ‘what does a risky unusual journey look like’. From here, we can unpick the intent of their website traffic, getting and staying ahead of the bad bots.”

Endpoint protection

When considering certain aspects of cyber security that can benefit from the technology, Tim Brown, vice-president of security architecture at SolarWinds says that AI can play a role in protecting endpoints. This is becoming ever the more important as the amount of remote devices used for work rises.

“By following best practice advice and staying current with patches and other updates, an organisation can be reactive and protect against threats,” said Brown. “But AI may give IT and security professionals an advantage against cyber criminals.

“Antivirus (AV) versus AI-driven endpoint protection is one such example; AV solutions often work based on signatures, and it’s necessary to keep up with signature definitions to stay protected against the latest threats. This can be a problem if virus definitions fall behind, either because of a failure to update or a lack of knowledge from the AV vendor. If a new, previously unseen ransomware strain is used to attack a business, signature protection won’t be able to catch it.

“AI-driven endpoint protection takes a different tack, by establishing a baseline of behaviour for the endpoint through a repeated training process. If something out of the ordinary occurs, AI can flag it and take action – whether that’s sending a notification to a technician or even reverting to a safe state after a ransomware attack. This provides proactive protection against threats, rather than waiting for signature updates.

“The AI model has proven itself to be more effective than traditional AV. For many of the small/midsize companies an MSP serves, the cost of AI-driven endpoint protection is typically for a small number of devices and therefore should be of less concern. The other thing to consider is how much cleaning up costs after infection – if AI-driven solutions help to avoid potential infection, it can pay for itself by avoiding clean-up costs and in turn, creating higher customer satisfaction.”

Machine learning versus SMS scams

With more employees working from home, and possibly using their personal devices to complete tasks and collaborate with colleagues more often, it’s important to be wary of scams that are afoot within text messages.

“With malicious actors recently diversifying their attack vectors, using Covid-19 as bait in SMS phishing scams, organisations are under a lot of pressure to bolster their defences,” said Brian Foster, senior vice-president of product management at MobileIron.

“To protect devices and data from these advanced attacks, the use of machine learning in mobile threat defence (MTD) and other forms of managed threat detection continues to evolve as a highly effective security approach.

“Machine learning models can be trained to instantly identify and protect against potentially harmful activity, including unknown and zero-day threats that other solutions can’t detect in time. Just as important, when machine learning-based MTD is deployed through a unified endpoint management (UEM) platform, it can augment the foundational security provided by UEM to support a layered enterprise mobile security strategy.

“Machine learning is a powerful, yet unobtrusive, technology that continually monitors application and user behaviour over time so it can identify the difference between normal and abnormal behaviour. Targeted attacks usually produce a very subtle change in the device and most of them are invisible to a human analyst. Sometimes detection is only possible by correlating thousands of device parameters through machine learning.”

Hurdles to overcome

These use cases and more demonstrate the viability of AI and cyber security staff effectively uniting. However, Mike MacIntyre, vice-president of product at Panaseer, believes that the space still has hurdles to overcome in order for this to really come to fruition.

“AI certainly has a lot of promise but as an industry we must be clear that its currently not a silver bullet that will alleviate all cyber security challenges and address the skills shortage,” said MacIntyre. “This is because AI is currently just a term applied to a small subset of machine learning techniques. Much of the hype surrounding AI comes from how enterprise security products have adopted the term and the misconception (willful or otherwise) about what constitutes AI.

"The algorithms embedded in many modern security products could, at best, be called narrow, or weak, AI; they perform highly specialised tasks in a single, narrow field and have been trained on large volumes of data, specific to a single domain. This is a far cry from general, or strong, AI, which is a system that can perform any generalised task and answer questions across multiple domains. Who knows how far away such a system is (there is much debate ranging from the next decade to never), but no CISO should be factoring such a tool in to their three-to-five year strategy.

"Another key hurdle that is hindering the effectiveness of AI is the problem of data integrity. There is no point deploying an AI product if you can't get access to the relevant data feeds or aren't willing to install something on your network. The future for security is data-driven, but we are a long way from AI products following through on the promises of their marketing hype."

07 Sep 2020

43 Automated benchmarking platform for Quantum Compilers

https://www.swissquantumhub.com/automated-benchmarking-platform-for-quantum-compilers/

Arline announced the release of Arline Benchmarks which is the first open-source automated benchmarking platform for quantum compilers! The name was given to the honour of Arline Greenbaum, the first wife of Richard Feynman, one of the greatest physicists of all times, the father of modern quantum mechanics and quantum computing.

Efficient compilation of quantum algorithms and circuit optimisation is vital in the era of noisy intermediate scaly noisy devices. While there are multiple quantum circuit compilation and optimisation frameworks available, such as **Qiskit** (IBM), **Pytket** (CQC), **Cirq** (Google), there is no good way to compare their performance. Understanding the performance of the compilation frameworks is essential for the design process of efficient and useful solutions for today real-life problems.

Arline Benchmarks solves this problem by providing the solution for cross-benchmarking of quantum compilers. The comparison of different quantum compilation frameworks is based on a set of relevant metrics, such as final gate count, circuit depth, compiler runtime etc. Moreover, Arline Benchmarks allows user to combine circuit compilation and optimisation routines from different providers in a custom compilation pipeline to achieve the best performance.

Arline Benchmarks is currently available as a free software in the public domain at Github.

04 Sep 2020

44 Quantum leap forward in cryptography could make niche technology mainstream

by Adam Bannister

https://portswigger.net/daily-swig/quantum-leap-forward-in-cryptography-could-make-niche-technology-mainstream

Scientists claim to have made a breakthrough in quantum cryptography that could make internet communications "impregnable" against cyber-attacks.

A team of researchers has developed a quantum communications network that could lower the price and complexity of building quantum key distribution systems.

This could transform an established but niche technology currently limited to use by banks and governments into something available to "millions of users in the not too distant future", according to Dr Siddarth Joshi, who led the study at Bristol University's Quantum Engineering Technology Labs.

"Until now, building a quantum network has entailed huge cost, time, and resource, as well as often compromising on its security which defeats the whole purpose."

Quantum solace

Quantum key distribution allows two parties to share a secret key used to encrypt and decrypt information. Any successful attempt to intercept the key by an eavesdropper would result in the corruption of the key being exchanged because of fundamental principles of quantum mechanics.

Any attempt to monitor the state of a quantum system must disturb it, introducing anomalies in the process that can be detected and used to abort a key exchange.

But while quantum key distribution has been deployed by banks in China and, back in 2007, to secure elections in Switzerland, their resource-intensity has precluded their general application.

"Until now efforts to expand the network have involved vast infrastructure and a system which requires the creation of another transmitter and receiver for every additional user.

"Sharing messages in this way, known as trusted nodes, is just not good enough because it uses so much extra hardware which could leak and would no longer be totally secure," said Dr Joshi.

The 'entanglement' principle

The new technique is designed to overcome this problem by leveraging the 'entanglement' principle, whereby two particles simultaneously interact with each other at vast distances from one another.

"This latest methodology, called multiplexing, splits the light particles, emitted by a single system, so they can be received by multiple users efficiently," said Dr Joshi.

The Bristol team's node-free prototype can sustain eight users with the same number of receiver boxes, compared to the 56 boxes that would be required using previously best available method of quantum key distribution.

And the gains in resource efficiency would only widen as networks are scaled up, the theory goes.

The researchers say that they built their network for £300,000 in a matter of months, while commercially available production systems might cost millions in comparison.

The system was road-tested in Bristol with receiver boxes connected at various points around the UK city's existing optical fibre network.

The end of MitM attacks?

Quantum key distribution is not based "on problems that are difficult to solve" like RSA, which "can be hacked with clever algorithms, powerful computers and enough time," Dr Joshi tells The Daily Swig.

"Implemented correctly", quantum key distribution leverages the laws of physics to ensure that "data being transmitted cannot be intercepted and hacked".

This could herald the end of manipulator-in-the-middle (MitM) attacks, says the researcher, even if threat actors build their own quantum systems and connect "into the path between" the sender and recipient.

"The no-cloning principle forbids the exact duplication of a quantum state and [attackers] will introduce errors and hence be detected."

The service would still be prone to denial of service – which "could be as simple as cutting the fibre with a scissor" – while encrypted communications could be leaked by data recipients or insecure endpoints.

However, entanglement-based quantum communication allows "end users to verify the quantum functionality of" devices. "Further, various device independent protocols exist which can ensure security even if some of the underlying quantum devices are compromised."

45 New technology lets quantum bits hold information for 10,000 times longer than previous record

by Tohoku University

https://www.sciencedaily.com/releases/2020/09/200904121331.htm

Quantum bits, or qubits, can hold quantum information much longer now thanks to efforts by an international research team. The researchers have increased the retention time, or coherence time, to 10 milliseconds – 10,000 times longer than the previous record – by combining the orbital motion and spinning inside an atom. Such a boost in information retention has major implications for information technology developments since the longer coherence time makes spin-orbit qubits the ideal candidate for building large quantum computers.

"We defined a spin-orbit qubit using a charged particle, which appears as a hole, trapped by an impurity atom in silicon crystal," said lead author Dr. Takashi Kobayashi, research scientist at the University of New South Wales Sydney and assistant professor at Tohoku University. "Orbital motion and spinning of the hole are strongly coupled and locked together. This is reminiscent of a pair of meshing gears where circular motion and spinning are locked together."

Qubits have been encoded with spin or orbital motion of a charged particle, producing different advantages that are highly demanded for building quantum computers. To utilize the advantages of qubits, Kobayashi and the team specifically used an exotic charged particle "hole" in silicon to define a qubit, since orbital motion and spin of holes in silicon are coupled together.

Spin-orbit qubits encoded by holes are particularly sensitive to electric fields, according to Kobayashi, which allows for more rapid control and benefits scaling up quantum computers. However, the qubits are affected by electrical noise, limiting their coherence time.

"In this work, we have engineered sensitivity to the electric field of our spin-orbit qubit by stretching the silicon crystal like a rubber band," Kobayashi said. "This mechanical engineering of the spin-orbit qubit enables us to remarkably extend its coherence time, while still retaining moderate electrical sensitivity to control the spin-orbit qubit."

Think of gears in a watch. Their individual spinning propels the entire mechanism to keep time. It is neither the spin nor orbital motion, but a combination of them that takes the information forward.

“These results open a pathway to develop new artificial quantum systems and to improve the functionality and scalability of spin-based quantum technologies,” Kobayashi said.

03 Sep 2020

46 Near-optimal chip-based photon source developed for quantum computing

by The Optical Society

https://phys.org/news/2020-09-near-optimal-chip-based-photon-source-quantum.html

Researchers have developed a new CMOS-compatible silicon photonics photon source that satisfies all the requirements necessary for large-scale photonic quantum computing. The research represents a significant step toward mass-manufacturable ideal single photon sources.

There is a widespread effort to develop chip-based quantum computers because the mature CMOS fabrication processes used to make today’s computer chips could greatly lower the cost of large-scale quantum information processing. Although researchers have demonstrated many of the components needed to make quantum computers in silicon chips, an on-chip single photon-source has proven challenging because of the stringent demand to create high-quality photons.

Stefano Paesani from the University of Bristol in the UK will present the new research at the all-virtual OSA Frontiers in Optics and Laser Science APS/DLS (FiO + LS) conference to be held 14-17 September.

“By demonstrating low-noise photon sources simultaneously meeting all requirements for large-scale photonic quantum computers, we have overcome a crucial challenge that had limited the scaling of quantum photonic technologies,” said Paesani. “The techniques developed in this work could speed up the development of mass-manufacturable chip-scale quantum technologies by several years. Such technologies promise enormous computational quantum speed-ups, unconditionally secure communications, and quantum-enhanced sensors.”

Creating quality photons

As the name implies, single-photon sources emit light as single photons. They are a key component of optical quantum computers, which use the photons to carry data in the form of qubits. Qubits can be in two states at the same time and will interfere, or correlate, with each other, allowing many processes to be performed simultaneously.

Single-photon sources used in quantum computing have very exacting requirements. They must be highly indistinguishable and pure, either near-deterministic or highly efficient, and suitable for mass-manufacturing. To meet all these requirements, Paesani and coworkers designed a new single-photon source based on inter-modal spontaneous four-wave mixing in a multi-mode silicon waveguide.

The inter-modal approach to on-chip photon sources, where an interplay between multiple optical pump fields is used to generate photons, enables novel degrees of freedom to control the photon emission. By tailoring the geometry of a low-loss multi-mode waveguide and the on-chip temporal delay between the pump fields, the research team showed that the properties of the spontaneous photon emission could be engineered to achieve near-ideal photons.

To test the new design, the researchers fabricated single-photon devices on standard silicon-on-insulator using CMOS-compatible lithography processes on a commercial wafer. Tests of the devices revealed that the multi-mode waveguides significantly reduced transmission losses, enabling an intrinsic heralding efficiency of the source of approximately 90%. A high heralding efficiency is necessary to scale up quantum processing.

The researchers also performed on-chip photon interference, which is essential for quantum computations. These experiments produced a raw-data visibility of 96%, the highest reported so far in integrated photonics. This achievement enables on-chip quantum operations between photons at an unprecedented level of precision, opening the possibility to scale-up low-noise photon processing in near-term quantum photonic devices.

The researchers say that the single-photon source could be further improved with a better pump laser and by using a more uniform fabrication process.

02 Sep 2020

47 Rigetti Computing to Lead £10M Consortium to Launch First Commercial Quantum Computer in UK

by Rigetti Computing

http://www.globenewswire.com/news-release/2020/09/02/2087495/0/en/Rigetti-Computing-to-Lead-10M-Consortium-to-Launch-First-Commercial-Quantum-Computer-in-UK.html

Rigetti UK announced today it will lead a £10 million consortium to accelerate the commercialisation of quantum computing in the UK. The three-year programme will build and operate the first quantum computer in the UK, make it available to partners and customers over the cloud, and pursue practical applications in machine learning, materials simulation, and finance. Rigetti is joined by Oxford Instruments, University of Edinburgh, quantum software start-up Phasecraft, and Standard Chartered Bank.

“Our ambition is to be the world’s first quantum-ready economy, which could provide UK businesses and industries with billions of pounds worth of opportunities,” said Science Minister Amanda Solloway. “Therefore, I am delighted that companies across the country will have access to our first commercial quantum computer, to be based in Abingdon. This is a key part of our plan to build back better using the latest technology, attract the brightest and best talent to the UK and encourage world-leading companies to invest here.”

Many industries central to the UK economy are poised to benefit from quantum computing, including finance, energy, and pharmaceuticals. A recent BCG report projected the global quantum industry to reach £4B by 2024.

“We are excited to deliver the UK’s first quantum computer and help accelerate the development of practical algorithms and applications.” said Chad Rigetti, CEO of Rigetti Computing. By providing access to quantum hardware, the collaboration aims to unlock new capabilities within the thriving UK ecosystem of quantum information science researchers, start-ups, and enterprises who have already begun to explore the potential impact of quantum computing.

Rigetti will build the superconducting quantum computer in a Proteox dilution refrigerator provided by Oxford Instruments. The University of Edinburgh will develop new ways of testing quantum hardware and verifying the performance of quantum programs, and will work with Standard Chartered Bank to advance quantum machine learning applications for finance. In addition, Phasecraft will use its deep knowledge of quantum algorithms and high-efficiency quantum software to harness this hardware for near-term applications in materials design, energy, and pharmaceuticals.

In addition to delivering a practical quantum computer in the UK, a key goal of the initiative is to further develop the country's quantum computing talent, infrastructure, and national supply chain, and to advance the high-performance computing industry.

"The UK is investing in quantum technologies not only to create society-changing products and services but also to grow talent and expertise, create new jobs and turn outstanding science into economic prosperity," said Roger McKinlay, challenge director for quantum technologies at UK Research and Innovation. "I am delighted that Rigetti – a global leader in quantum computing – have chosen to invest in the UK through this project, building on the close relationships they have already forged with UK companies and research organisations."

The consortium is backed by £10 million government and industry investment, including funding from the government's Quantum Technologies Challenge, led by UK Research & Innovation.

48 Next-generation encryption: What it will look like, and why we'll need it

by Frank Ohlhorst

https://www.hpe.com/us/en/insights/articles/next-generation-encryption--what-it-will-look-like-and-why-we-ll-need-it-2009.html

The next generation of computing – think quantum and beyond – could soon threaten current asymmetric encryption technologies, including PKI. Here's what you need to know.

Threats to current encryption techniques are on the horizon. The National Institute of Standards (NIST) predicts that within the next few years, the most credible of these technologies, sufficiently capable quantum computers, will become a viable threat. The concern is that these systems will be built to break essentially all asymmetric encryption schemes in use, effectively rendering public key infrastructure (PKI) encryption useless.

While fully functional quantum computers may still be several years away, recent technological strides potentially have accelerated the timeline. Advances include the claim that researchers have achieved quantum supremacy, where a quantum computer can perform a calculation beyond the capability of even the currently most powerful classical supercomputers.

Quantum computing algorithms that are a threat to public key encryption, or asymmetric encryption algorithms, have been developed. One bright spot is that symmetric encryption algorithms, such as Advanced Encryption Standard (AES), are thought to be more resistant to quantum computing algorithms, and an efficient quantum computing algorithm is not yet known to break these encryption technologies.

This means that protocols that use asymmetric algorithms at any point are vulnerable. It is why a state actor could capture all Transport Layer Security (TLS) traffic in the hope of one day being able to decrypt the data. This would likely be too expensive for cybercriminals – currently, the costs outweigh the benefits.

If the scientific world is that much closer to building a fully functional quantum computer, cybersecurity specialists may need to start rethinking how encryption will work in a post-quantum computing world. This is the goal of the process NIST has initiated to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.

Post-quantum cryptography: The coming standards

Preparing for the worst-case scenario, even with the unlikelihood of it becoming an issue in the near term, NIST recognizes the importance of post-quantum cryptography (PQC), stating, "Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing."

To that end, NIST has been requesting submissions for PQC standards and working with industry leaders to come up with a methodology to address the future threats posed by quantum computing-powered attacks. That process has recently entered round three, where proposed PQC algorithms will be further evaluated for their resiliency against quantum computers. The third-round finalists may very well set the stage for what will become a set of standards for PQC and redefine how PKI, digital signatures, and other encryption techniques are deployed.

Keep security current by looking ahead

Although new NIST standards are being worked out, businesses can still ready themselves for when the need for these standards becomes a reality. Potentially, the threats are imminent, and cybercriminals may already be hoarding encrypted data in the hope of using quantum computers to break into that data. Experts from numerous digital security firms, such as DigiCert, Gemalto, Ultimaco, and several others, are offering intelligence and advice on how to prepare for a post-quantum world. While most point to their own services or products, all agree to several basic ideas in the quest to ready businesses for a post-quantum world:

- **Improve crypto-agility:** Crypto-agility, as the name implies, is the process of identifying and managing cryptographic algorithms. Pretty much any connected organization uses some type of crypto, and if it is using a secure environment, there is some type of cryptography involved. Organizations must identify every element – such as servers, protocols, libraries, algorithms, and certificates that utilize encryption – and then be able to manage those. The key here is to be able to manage the lifecycle of crypto technologies. Organizations can turn to a certificate management platform to achieve much of that. It is also critical to create a plan about how to identify and resolve encryption issues, such as expired certificates or weak algorithms. Once all crypto resources are identified, organizations will need to work with their third-party vendors to determine how those vendors plan to protect against quantum threats.
- **Catalog all hardware security modules (HSMs):** Many organizations use HSMs to safeguard and manage digital keys. HSMs also perform encryption and decryption functions for digital signatures, strong authentication, and other cryptographic functions. Most important, HSMs are often found in card payment systems or smart card access systems and are becoming ubiquitous in many organizations. It is critical to identify all HSMs, understand how they are being used, and determine if the

HSMs can be upgraded to support the next set of threats to encryption. That will require contacting the HSM vendors and verifying if there is an upgrade or replacement path.

- **Maintain best practices for TLS deployments:** These are the most vulnerable points of attack in the post-quantum encryption world. Best practices will keep you on the leading edge of security and encryption updates. When somebody builds a viable quantum computer, we'll all need to upgrade our TLS libraries.

- **Have a plan and test it:** Identifying the parts and pieces that are subject to a quantum threat is only the beginning of a plan. Organizations will also need to define what to do if a potential threat is encountered, which is already a best practice in the realm of cybersecurity. The key here is to identify critical elements and build a plan that addresses those elements. The plan should also be frequently tested. For example, if an organization is notified of a certificate compromise, it may want to be immediately ready to deploy a replacement certificate, and the only way to be fully ready is to have tested such a scenario in the first place. Many organizations create sandboxes or build non-production test systems for the purpose of validating changes before applying those changes to a production network.

Next-generation computing technologies and quantum computing present threats to the current encryption technologies in place. However, the most ominous threat may not materialize for some time, with some experts suggesting that a fully functioning quantum computer could still be decades away while others claim that quantum computing will become viable in just a few short years. Either way, there is no harm in preparing for the next generation of hardware threats now instead of later. After all, improving one's crypto-agility offers real-world benefits today and helps to mitigate current cybersecurity attack vectors while helping organizations to be more prepared for other threats as well.

49 A molecular approach to quantum computing

by Whitney Clavin

https://phys.org/news/2020-09-molecular-approach-quantum.html

The technology behind the quantum computers of the future is fast developing, with several different approaches in progress. Many of the strategies, or "blueprints," for quantum computers rely on atoms or artificial atom-like electrical circuits. In a new theoretical study in the journal Physical Review X, a group of physicists at Caltech demonstrates the benefits of a lesser-studied approach that relies not on atoms but molecules.

"In the quantum world, we have several blueprints on the table and we are simultaneously improving all of them," says lead author Victor Albert, the Lee A. DuBridge Postdoctoral Scholar in Theoretical Physics. "People have been thinking about using molecules to encode information since 2001, but now we are showing how molecules, which are more complex than atoms, could lead to fewer errors in quantum computing."

50 Revolutionary quantum breakthrough paves way for safer online communication

by University of Bristol

https://phys.org/news/2020-09-revolutionary-quantum-breakthrough-paves-safer.html

The world is one step closer to having a totally secure internet and an answer to the growing threat of cyber-attacks, thanks to a team of international scientists who have created a unique prototype which could transform how we communicate online.

The invention led by the University of Bristol, revealed today in the journal Science Advances, has the potential to serve millions of users, is understood to be the largest-ever quantum network of its kind, and could be used to secure people's online communication, particularly in these internet-led times accelerated by the COVID-19 pandemic.

By deploying a new technique, harnessing the simple laws of physics, it can make messages completely safe from interception while also overcoming major challenges which have previously limited advances in this little used but much-hyped technology.

Lead author Dr. Siddarth Joshi, who headed the project at the university's Quantum Engineering Technology (QET) Labs, said: "This represents a massive breakthrough and makes the quantum internet a much more realistic proposition. Until now, building a quantum network has entailed huge cost, time, and resource, as well as often compromising on its security which defeats the whole purpose."

"Our solution is scalable, relatively cheap and, most important of all, impregnable. That means it's an exciting game changer and paves the way for much more rapid development and widespread rollout of this technology."

The current internet relies on complex codes to protect information, but hackers are increasingly adept at outsmarting such systems leading to cyber-attacks across the world which cause major privacy breaches and fraud running into trillions of pounds annually. With such costs projected to rise dramatically, the case for finding an alternative is even more compelling and quantum has for decades been hailed as the revolutionary replacement to standard encryption techniques.

So far physicists have developed a form of secure encryption, known as quantum key distribution, in which particles of light, called photons, are transmitted. The process allows two parties to share, without risk of interception, a secret key used to encrypt and decrypt information. But to date this technique has only been effective between two users.

51 Xanadu launches quantum cloud platform, plans to double qubits every 6 months

by Emil Protalinski

https://venturebeat.com/2020/09/02/xanadu-photonics-quantum-cloud-platform/

Quantum computing startup Xanadu today launched its quantum cloud platform. Developers can now access Xanadu's gate-based photonic quantum processors with 8-qubit or 12-qubit chips – 24-qubit chips will be available "in the next month or so," Xanadu founder and CEO Christian Weedbrook told VentureBeat. The startup expects to "roughly double" the number of qubits available in its cloud every six months. The hope is Xanadu Quantum Cloud will let businesses, developers, and researchers build novel solutions to problems in finance, quantum chemistry, machine learning, and graph analytics.

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 for a classical computer. Based in Toronto, Canada, Xanadu has been developing quantum computers based on photonics since its founding in September 2016. The choice of technology means Xanadu's quantum processors operate at room temperature (most other examples of quantum computing tech have to be cooled to very low temperatures) and can be integrated into existing fiber optic-based telecommunication infrastructure.

Xanadu is best known for the development of **PennyLane**, an open source software library for quantum machine learning, quantum computing, and quantum chemistry. The company also develops Strawberry Fields, its cross-platform Python library for simulating and executing programs on quantum photonic hardware. Both open source tools are available on GitHub, and they have a growing community fostering tutorials and educational materials for anyone interested in developing and experimenting with quantum applications.

"PennyLane, which you can think of as a TensorFlow for quantum computing, actually runs on not only our hardware but everyone else's hardware, which is really cool," Weedbrook told VentureBeat. "A lot of people love PennyLane, and there's a strong brand recognition with Xanadu there. The ability to run on many things, I think that will also draw people back to our cloud."

52 The UK is building its first commercial quantum computer

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/the-uk-is-building-its-first-commercial-quantum-computer/

The UK's splashing the cash for its next quantum purchase: the science minister Amanda Solloway has announced the country's very first commercial quantum computer, backed by a £10 million investment from government and industry, to be available to use by businesses within the next few years.

The new machine is expected to help businesses unleash the billion-dollar opportunities promised by the quantum revolution in industries ranging from pharmaceuticals and transport to aerospace.

While the new quantum computer will be physically located in Abingdon, Oxfordshire, partners and customers will be able to access and operate the system over the cloud, to run applications in machine learning, materials simulation and finance.

Solloway said: "Our ambition is to be the world's first quantum-ready economy, which could provide UK businesses and industries with billions of pounds worth of opportunities. Therefore, I am delighted that companies across the country will have access to our first commercial quantum computer, to be based in Abingdon."

California-based company Rigetti Computing will develop the quantum computer over a three-year programme, in partnership with various UK organizations such as the University of Edinburgh, Oxford Instruments, Standard Chartered Bank and Phasecraft.

Rigetti was one of the 38 winners of the Quantum Technologies Challenge last June, a competition led by UK Research and Innovation (UKRI) that rewards projects focused on commercialising quantum technologies. The funding received as part of the challenge will be used to lead the development of the new quantum computer in Abingdon.

The US company is one of the only businesses developing quantum computing platforms around the world. Rigetti builds quantum computers and the superconducting quantum processors that power them, and then operates the technology in tandem with classical computing resources on a platform called Quantum Cloud Services (QCS), so that the quantum machines can be integrated into a public, private or hybrid cloud.

After the quantum computer is built, complete with superconducting quantum processors and chips, the device is housed in very low-temperature dilution refrigerators to enable better control of the qubits. The hardware can then operate on the QCS platform, and third parties can access the machine using classical computing resources over the cloud.

Rigetti's superconducting qubit technology will be used to build the quantum computer in Oxfordshire, and the device will be housed in a dilution refrigerator provided by Oxford Instruments. The University of Edinburgh will develop new ways of testing the hardware and the performance of the programmes. Standard Chartered Bank will work on applications of the technology for finance, while Phasecraft will look at quantum algorithms for materials design, energy, and pharmaceutical.

The consortium plans to have the quantum computer operable in the second half of next year, and to continue to improve its scale and performance throughout the lifetime of the project and beyond.

"By providing access to quantum hardware, the collaboration aims to unlock new capabilities within the thriving UK ecosystem of quantum information science researchers, start-ups, and enterprises who have already begun to explore the potential impact of quantum computing," said Chad Rigetti, the CEO of Rigetti Computing.

Given the cost and complexity of building a standalone quantum computer for one single application, many organisations are turning to hybrid models and shared resources, an approach that Rigetti is pushing forward with QCS.

The US company is competing against tech giants like IBM in the quest to commercialise quantum computing at scale. Last year, for example, IBM launched its own commercial quantum computer, called IBM Q System One. The device exists as a physical 20-qubit computer that can be purchased as a piece of hardware; or, it can be accessed by developers over the cloud, as part of a network called "Q Network".

Since the Q System One was released, the company has deployed 15 devices for laboratories and companies to rent for use in research. The Q Network, for its part, has over 100 members and has run more than 130 billion executions since the programme started.

Flexible access to quantum hardware, while using familiar classical resources, is an attractive prospect for businesses. Quantum computers, when they are commercially available, are expected to provide better and quicker ways to solve problems such as optimising financial portfolios, improving AI computations or discovering new drugs to treat neurodegenerative diseases.

The UK has vowed to remain at the forefront of quantum research, and has already invested £1 billion in a ten-year national programme designed to boost quantum technologies.

As part of the national programme, the UK government also launched the National Quantum Computing Centre (NQCC), a £93 million venture announced two years ago to improve the commercialization of quantum technologies, and provide businesses and research institutions with access to quantum computers as they are developed around the world.

Now halfway through the national programme, however, it is emerging that scaling up the huge potential of quantum computing is as hard as it sounds. While quantum research is taking leaps, industrial applications are effectively taking time to emerge.

Speaking at a conference earlier this year in London, Elham Kashefi, chair in quantum computing at the University of Edinburgh, said: "The UK has a very strong lead in research (...). We have the base but I don't know how we can create the money to push it to the next level, to connect to industry. There is a gap, because we need everything that is achieved in the national programme to be connected to the industry."

Providing businesses and organisations with access to a quantum computer, therefore, could significantly accelerate the development of practical applications for quantum, and bring about a deluge of innovation as the technology comes out of the lab and into the real world.

53 A 8.5 GHz Quantum Analyzer by Zurich Instruments

https://www.swissquantumhub.com/8-5-ghz-quantum-analyzer-by-zurich-instruments/

The Swiss company Zurich Instruments has just introduced its SHFQA Quantum Analyzer that operates at up to 8.5 GHz and can thus perform direct readout of superconducting and spin qubits.

Conceived as the next generation of quantum computing instrumentation, the SHFQA combines signal generation at microwave frequencies with direct qubit readout and real-time multi-state discrimination.

With the SHFQA, reading out frequency-multiplexed qubits on up to 4 readout lines becomes a fast, high-fidelity operation that does not rely on tedious mixer calibration. As a single SHFQA can measure up to 64 qubits (or 32 qutrits or 20 ququads), it covers many functionalities that would otherwise require larger instrument racks and complex cabling arrangements.

As part of the Quantum Computing Control System (QCCS), the SHFQA is seamlessly integrated into new or existing setups featuring the HDAWG Arbitrary Waveform Generator and the PQSC Programmable Quantum System Controller. The LabOne user interface already known to Zurich Instruments' customers gives access to an overview of all settings on the instrument, from the readout-band center frequency to the configuration of the low-latency analysis chain.

54 Hardware-aware approach for fault-tolerant quantum computation

by Guanyu Zhu and Andrew Cross

https://www.ibm.com/blogs/research/2020/09/hardware-aware-quantum/

Although we are currently in an era of quantum computers with tens of noisy qubits, it is likely that a decisive, practical quantum advantage can only be achieved with a scalable, fault-tolerant, error-corrected quantum computer. Therefore, development of quantum error correction is one of the central themes of the next five to ten years. Our article "Topological and subsystem codes on low-degree graphs with flag qubits", published in Physical Review X, takes a bottom-up approach to quantum error correcting codes that are adapted to a heavy-hexagon lattice – a topology that all our new premium quantum processors use, including IBM Quantum Falcon ($d = 3$) and Hummingbird ($d = 5$).

A bottom-up approach

Many in the quantum error correction community pursue a top-down computer science approach, i.e., designing the best codes from an abstract perspective to achieve the smallest logical error rate with minimal resource. Along this path, the surface code is the most famous candidate for near-term demonstrations (as well as mid- to long-term applications) on a two-dimensional quantum computer chip. The surface code naturally requires a two-dimensional square lattice of qubits, where each qubit is coupled to four neighbors.

We started with the surface code architecture on our superconducting devices and demonstrated an error detection protocol[2] as a building block of the surface code around 2015. While the experimental team at IBM made steady progress with cross-resonance (CR) gates, achieving gate fidelities near 99%, an experimental obstacle appeared along the path of scaling up the surface code architecture. The specific way to operate the CR gates requires the control qubit frequency to be detuned from all its neighboring target qubits, such that the CNOT gates between any pair of control and target can be individually addressed.

The significant experimental challenges posed by this and other frequency constraints was a sign that the traditional top-down approach would need to be revised.

Due to the fixed, narrow windows of allowed frequencies for the superconducting qubits, a greater number of assigned frequencies lowers the success rate to fabricate chips, given that there are inevitable random fluctuations during fabrication. CR gates are best matched to a layout where qubits are located on the vertices of a low-degree graph, such as the so-called “heavy-hexagon” lattice pursued by our team. For example, IBM’s current device topology implements a heavy-hexagon lattice as shown in Fig. 1(a), where qubits are located on the nodes and edges of each hexagon. Each qubit has either two or three neighbors, meaning the graph has vertices of degree-2 or -3. As a consequence, only three different frequency assignments are necessary, which are shown as three different colors in Fig. 1(b), as opposed to a square lattice, which naturally requires at least five different frequencies for addressability. The heavy-hexagon lattice also greatly reduces crosstalk errors since, in principle, only qubits on the edges of the lattice need to be driven by CR drive tones.

This led us to ask the following questions: what quantum error correcting codes are hardware-optimal, in the sense that they are adapted to the heavy-hexagon lattice? To what degree can quantum error-correcting codes be hardware-aware?

Guided by this bottom-up principle, we developed two new classes of codes: subsystem codes called heavy-hexagon codes implemented on a heavy-hexagon lattice, and heavy-square surface codes implemented on a heavy-square lattice.

The IBM team is currently implementing these codes on the new quantum devices.

Constraints lead to art

One might think that hardware constraints will limit the creativity of code design, but what has happened is quite the opposite. Similar to the surface code, the new codes also require a 4-body syndrome measurement, as shown in the following figure, where four qubits on the legs could be measured by coupling them to a central auxiliary qubit.

[2] A. D. Córcoles, E. Magesan, S. J. Srinivasan., A. W. Cross, M. Steffen, J. M. Gambetta & J. M. Chow, Demonstration of a quantum error detection code using a square lattice of four superconducting qubits, Nat Commun 6, 6979 (2015).

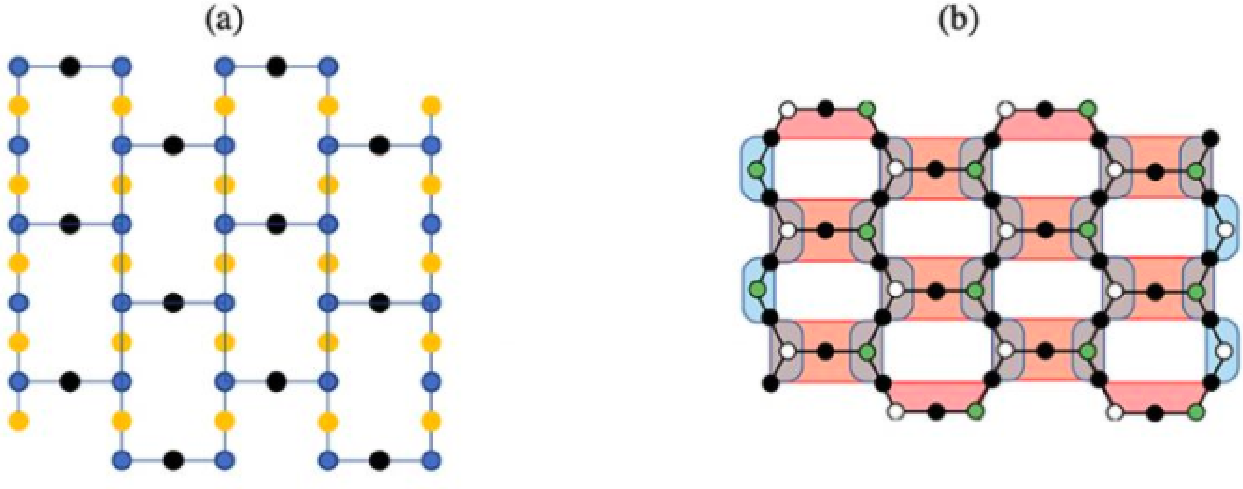
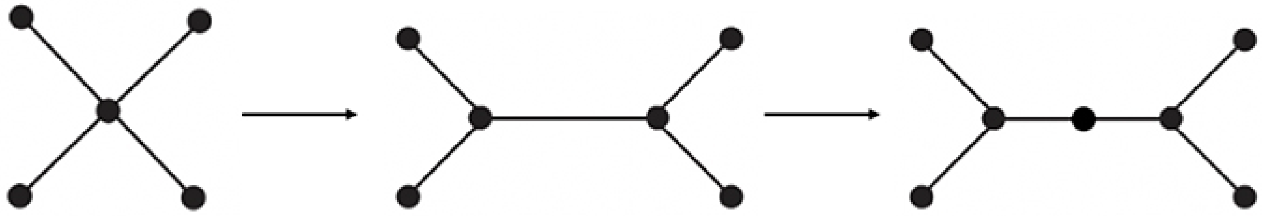


Fig. 1: (a) IBM Quantum's 65-qubit topology design uses a heavy-hexagon lattice. (b) Illustration of the frequency assignments for implementing the cross-resonance gates on the heavy-hexagon lattice.



To measure such a 4-body syndrome, we split the central vertex into two vertices, inserting auxiliary qubits for each, and successfully reduce the graph to degree-3. By adding another vertex (qubit) in the middle, we can measure the 4-body syndrome on the heavy-hexagon lattice with a mixture of degree-3 and -2 vertices. Meanwhile, the two extra qubits now function as so-called flag qubits, which can be used to significantly suppress error propagation in the measurement circuit.

Development of a corresponding decoder that can use this flag information is also part of the fault-tolerant quantum computing scheme. As a consequence, we have found competitive error-correcting codes and circuits, despite a constrained hardware layout. Perhaps even more intriguing is that the heavy-hexagon code belongs to a family of subsystem codes that is a hybrid of the surface code and the Bacon-Shor code, both of which are famous and widely studied examples in the quantum error correction community.

Although it might seem contradictory, constraints can lead to artistic creativity and freedom. Examples of amazing art emerging from constrained media are too numerous to name here, so we offer just two.

Bach's Fugues exhibit counterpoint that constrains the melodic interactions of several melodies in such a way that they become beautiful polyphony when played together. Michael Keith's 1995 poem "Near a Raven" is a retelling of Edgar Allen Poe's eponymous poem in more than 700 words, wherein word lengths are constrained to be the digits of pi.

IBM scientists are similarly working together within the constraints of physics to create quantum computing devices, leading to qubit arrangements such as the heavy-hexagon lattice and subsequent enrichment of the family of existing quantum codes.

Co-design of quantum hardware and error-correcting codes

This hardware-aware, bottom-up approach provides a bridge between more abstract theory and practical quantum engineering. We have seen one example of how physical constraints can influence implementations of quantum error correction. This is an example of co-design, specifically of quantum hardware, error-correcting codes, and fault-tolerant operations. In essence, we willfully break abstraction layers to create more practical and better optimized microarchitectures for quantum computers.

Another example of co-design is when abstract error-correction theory suggests requirements for optimal hardware. The tension between ideal requirements and physical constraints couples the abstract and the practical. The concept of co-design in quantum engineering is likely to grow in importance as we move closer as a community to experimentally demonstrating fault-tolerant quantum error correction.

01 Sep 2020

55 Quantum Computing May Be Closer Than You Think

by Dario Gil

https://www.scientificamerican.com/article/quantum-computing-may-be-closer-than-you-think/

Fully functional quantum computers and a new quantum industry may appear much sooner than many have anticipated – thanks to five new National Quantum Information Science Research centers just announced by the U.S. Department of Energy. This latest development in the recently launched National Quantum Initiative Act, signed into law in December 2018, comes with $625 million in funding over five years.

It's a huge deal: for the first time, researchers from academia, U.S. national labs and industry will be working side by side aiming to speed up the fundamental quantum information science research. And more research should bring us closer to advanced quantum technologies and the grandest goal of quantum information science, creating a fault-tolerant quantum computer that can indefinitely compute without errors.

Why do we need quantum computers? We need them to speed up the process of scientific discovery so that we can address some our greatest global challenges, from designing new materials for more efficient carbon capture plants and batteries to better drugs and vaccines. Traditionally, material design has depended a lot on either happy accidents or a long and tedious iterative process of experimentation. Over the past half a century, classical computers have greatly accelerated this process by performing molecular simulations. Still, classical computers can't simulate complex molecules with enough accuracy, and that's where quantum computing will be able to help.

Quantum computers rely on the same physical rules as atoms to manipulate information. Just like traditional, classical, computers execute logical circuits to run software programs, quantum computers use the physics phenomena of superposition, entanglement and interference to execute quantum circuits. One day soon, they should be able to perform mathematical calculations out of the reach of the most advanced current and future classical supercomputers.

But to get there, we will need to build quantum machines that compute without errors. Quantum computers rely on fragile qubits, short for quantum bits, which are only of use when they are in a delicate quantum state. Any external disturbances or "noise," such as heat, light or vibrations, inevitably yanks these qubits out of their quantum state and turns them into regular bits.

Overcoming this hurdle is beyond the limits of a single team, and we need scores of scientists from academia, the national labs and industry to get us there. This is where the new centers come in. At last, they will get the talent from all our R&D sectors to work together on quantum-related issues.

Take the problem of building a quantum system that would compute without errors. Our best theories estimate that to get there, we should build machines with tens of millions of qubits on a single cooled-down chip. But we don't want to cool down quantum chips the size of football fields. To avoid it, we need many breakthroughs – meaning we have to invest in research at scale. Luckily, some of the latest results show that it's possible to reduce the number of qubits we need to implement error-correcting codes.

But even if we achieve this, we will have to overcome another hurdle: linking quantum processors, just like we connect today's computer chips inside data centers using intranets. This requires quantum interconnects that transfer the fragile quantum information stored in the processor's qubits into a different quantum format (say, photons) that "communicate" the data to another processor. Advances in this space must unite disparate technologies like superconducting qubits and fiber optics, while solving outstanding challenges in materials science and quantum communications.

Research teams could probably solve these problems, and many other challenges the quantum information science community is tackling, individually. But it would take decades, and we can't afford to wait this long. Partnerships and collaboration, through the new centers, will offer us the chance of making the quantum leap we need. With a long-term vision of establishing a robust national quantum ecosystem, academia, national labs and industry partners at last have a quantum roadmap.

Now it's up to all the partners in this joint effort to create a quantum ecosystem and industry. We'll need plenty of the wit, talent, creativity and enthusiasm of a skilled and diverse quantum workforce to make it happen.

56 Google Team Completes First Successful Chemical Simulation on Quantum Computer

by Sandipan Talukdar

https://www.newsclick.in/google-team-completes-first-successful-chemical-simulation-quantum-computer

A complete chemical simulation on a quantum computer has been reported for the first time by the team working on Google's AI (Artificial Intelligence) quantum team. The team was successful in completing the chemical simulation on **Sycamore**, Google's quantum computer. The report published in Science says that the chemical simulation of a diazene molecule reacting with hydrogen atoms resulted in an altered configuration.

The hard part in the exercise was to make sure that the results were accurate. Quantum computers are very prone to errors, so validation was the challenge. To do this, the team paired the quantum computing facility with that of a classical computer, that is the computers we use in our day to day activities. The classical computing part was used to analyse the results provided by the sycamore quantum computer. Then new parameters were added and the process was repeated until the quantum computer could find a minimum value. Apart from this, the team used other checking systems as well to analyse the results produced by the quantum computer and to fix the errors.

In order to understand what is simulation, we need to first understand how a diazene molecule undergoes a change in its conformation, technically termed as the isomerisation of the molecule. To determine various aspects, say changes in angle, planarity etc. of a diazene molecule while undergoing the conformational changes, simulation technique could be used. Suppose at an initial time, say t_1, the molecule exists at a particular conformational state with specific angles between atoms. With time, the molecule reacts with other atoms such as the hydrogen atom and this eventually brings in changes in its previous state. Now, for the simulation, a computer is fed through coding with information about various parameters of the system of study and their interaction. Computer simulation is now used in almost all fields of scientific investigation, prediction of market status etc. But, for a very complex physical system, or a chemical system, carrying out such a simulation is very time consuming and also tedious. Quantum computers, however, may be able to perform the simulation in order to lessen the time of a complicated and long simulation done on the classical computing facility.

It should be noted that what Google has reported now, should be observed in continuation to its last year's report.

Last year, around the same time, Google's quantum computing facility was in the spotlight. A leaked paper had saidthat Google had achieved the so-called quantum supremacy. Google's 53 qubit computer could solve a problem in just 200 seconds, which otherwise would have taken some 10,000 years on a classical computer. The news was hyped to a great extent. The sycamore signified a narrow definition of quantum supremacy where the quantum computer is programmed to solve a highly specific task and there it can beat all other classical computers.

The latest simulation done by Sycamore is also specifically targeted for solving a particular problem. in other words, it's a successful trial to solve a standardised chemistry problem.