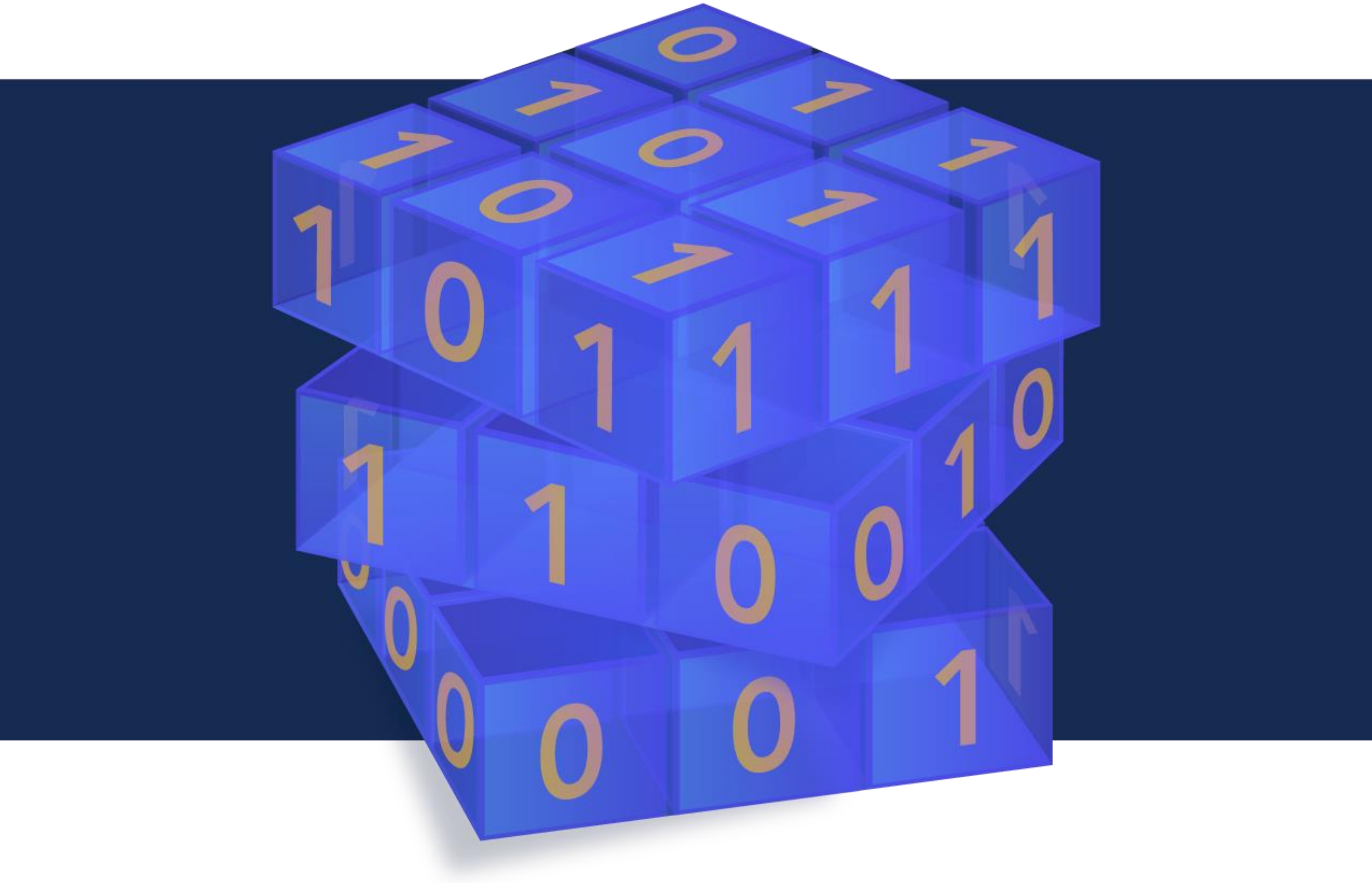
Crypto News

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

November 01, 2021



Contents

1.Editorial

SEATTLE, WA – November, 1st, 2021. We're keeping the excitement going with this month's Crypto News! What better way to start our journey than to ask the most basic question – Why do we care about quantum computers at all? Scroll down to article 22 to gain some insight. What do you think? Are quantum computers worth the hype? For those interested in sustainability, take some time to read article 6. A prototype of a compact quantum computer has been developed that shows the potential to be run on solar power. What an exciting proposition! The future is looking even brighter for quantum computing! So the next logical question becomes, is society thinking ahead and setting up our children and the quantum computing world for success? The quantum computing industry requires professionals who can write algorithms that solve complex problems. At the most basic level, quantum computing algorithms require an understanding of linear algebra and probabilities. Take a look at article 36 and judge for yourself. Will we have enough professionals in the future with the skills required to enter and thrive in the quantum computing industry?

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

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

2.Innovative Chip Resolves Quantum Headache – Paves Road to Supercomputer of the Future

by UNIVERSITY of COPENHAGEN
https://scitechdaily.com/innovative-chip-resolves-quantum-headache-paves-road-to-supercomputer-of-the-future/

Quantum physicists at the University of Copenhagen are reporting an international achievement for Denmark in the field of quantum technology. By simultaneously operating multiple spin qubits on the same quantum chip, they surmounted a key obstacle on the road to the supercomputer of the future. The result bodes well for the use of semiconductor materials as a platform for solid-state quantum computers.

One of the engineering headaches in the global marathon towards a large functional quantum computer is the control of many basic memory devices – *qubits* – simultaneously. This is because the control of one qubit is typically negatively affected by simultaneous control pulses applied to another qubit. Now, a pair of young quantum physicists at the University of Copenhagen’s Niels Bohr Institute – PhD student, now Postdoc, Federico Fedele, 29 and Asst. Prof. Anasua Chatterjee, 32, – working in the group of Assoc. Prof. Ferdinand Kuemmeth, have managed to overcome this obstacle.

Global qubit research is based on various technologies. While Google and IBM have come far with quantum processors based on superconductor technology, the UCPH research group is betting on semiconductor qubits – known as *spin qubits*.

“Broadly speaking, they consist of electron spins trapped in semiconducting nanostructures called quantum dots, such that individual spin states can be controlled and entangled with each other,” explains Federico Fedele.

Spin qubits have the advantage of maintaining their quantum states for a long time. This potentially allows them to perform faster and more flawless computations than other platform types. And, they are so minuscule that far more of them can be squeezed onto a chip than with other qubit approaches. The more qubits, the greater a computer’s processing power. The UCPH team has extended the state of the art by fabricating and operating four qubits in a 2×2 array on a single chip.

Circuitry is ‘the name of the game’

Thus far, the greatest focus of quantum technology has been on producing better and better qubits. Now it’s about getting them to communicate with each other, explains Anasua Chatterjee:

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

It is here that the young quantum physicists ’quantum circuit, made from the semiconducting substance gallium arsenide and no larger than the size of a bacterium, makes all the difference:

“The new and truly significant thing about our chip is that we can simultaneously operate and measure all qubits. This has never been demonstrated before with spin qubits – nor with many other types of qubits,” says Chatterjee, who is one of two lead authors of the study, which has recently been published in the journal *Physical Review X Quantum*.

Being able to operate and measure simultaneously is essential for performing quantum calculations. Indeed, if you have to measure qubits at the end of a calculation – that is, stop the system to get a result – the fragile quantum states collapse. Thus, it is crucial that measurement is synchronous, so that the quantum states of all qubits are shut down simultaneously. If qubits are measured one by one, the slightest ambient noise can alter the quantum information in a system.

Milestone

The realization of the new circuit is a milestone on the long road to a semiconducting quantum computer.

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

At the moment, one of the main challenges is that the chip's 48 control electrodes need to be tuned manually, and kept tuned continuously despite environmental drift, which is a tedious task for a human. That's why his research team is now looking into how optimization algorithms and machine learning could be used to automate tuning. To allow fabrication of even larger qubit arrays, the researchers have begun working with industrial partners to fabricate the next generation of quantum chips. Overall, the synergistic efforts from computer science, microelectronics engineering, and quantum physics may then lead spin qubits to the next milestones.

3.EMVCo adds support for elliptic curve cryptography

by Tom Phillips
https://www.nfcw.com/whats-new-in-payments/emvco-adds-support-for-elliptic-curve-cryptography/

EMVCo has issued a new specification bulletin that adds support for elliptic curve cryptography (ECC) to its EMV contact chip specifications to enable "robust EMV contact chip security long term as payment technologies evolve".

The addition of support for ECC is detailed in **Specification Bulletin 243** and applies to the EMV Integrated Circuit Card Specifications for Payment Systems v4.3.

Use of the ECC cryptography standard enables enhanced transaction security "without impacting on the technical performance of a payment device or slowing transaction processing time," the standards body says.

"In an EMV contact chip payment, the merchant point-of-sale terminal can cryptographically authenticate a card and its data.

"For this purpose, EMVCo has based its EMV contact chip specifications on RSA (Rivest-Shamir-Adleman) public key cryptography since its inception and intends to continue to support this standard.

"The addition of ECC into EMV specification helps achieve superior cryptographic strength with much smaller key sizes, enabling more efficient transactions in the future."

"The longer the cryptographic key used to secure a transaction, the more storage and processing power required. The size of a cryptographic key is therefore important," EMVCo Executive Committee chair Robin Trickel explains.

"EMVCo recognises that RSA could continue to offer 'stronger 'keys, however, these would increase in length resulting in slower computing and transaction times.

"In contrast, ECC is compact and efficient, making it an appealing option for use in devices with limited storage and processing capabilities.

"While it doesn't make current payments more secure today, it ensures robust security can be maintained in new payment innovations, setting the foundation to support the long-term security needs of the payment community."

4.Computing secure key rates for quantum cryptography with untrusted devices

by Ernest Y.-Z. Tan, René Schwonnek, Koon Tong Goh, Ignatius William Primaatmaja & Charles C.-W. Lim
https://www.nature.com/articles/s41534-021-00494-z

Device-independent quantum key distribution (DIQKD) provides the strongest form of secure key exchange, using only the input–output statistics of the devices to achieve information-theoretic security. Although the basic security principles of DIQKD are now well understood, it remains a technical challenge to derive reliable and robust security bounds for advanced DIQKD protocols that go beyond the previous results based on violations of the CHSH inequality. In this work, we present a framework based on semidefinite programming that gives reliable lower bounds on the asymptotic secret key rate of any QKD protocol using untrusted devices. In particular, our method can in principle be utilized to find achievable secret key rates for any DIQKD protocol, based on the full input–output probability distribution or any choice of Bell inequality. Our method also extends to other DI cryptographic tasks.

5.HTTPS threats grow more than 314% through 2021: Report

by Jonathan Greig
https://www.zdnet.com/article/https-threats-grow-more-than-314-through-2021-report/

Cybersecurity firm Zscaler has released their latest State of Encrypted Attacks Report, highlighting the growth in HTTPS threats since January as well as other attacks facing tech companies and retailers.

The report found that HTTPS threats have increased by more than 314% while attacks on tech companies grew by 2300% and retail companies saw an 800% increase in attacks. According to the report, the tech industry accounted for 50% of all attacks they tracked. Instances of malware were up 212% in the report and phishing rose by 90%.

The report tracks more than 20 billion threats blocked over HTTPS and analyzes about 190 billion daily transactions through its Zero Trust Exchange that took place from January to September. From there, the Zscaler ThreatlabZ research team goes through the data to compile the report.

Deepen Desai, CISO at Zscaler, said most enterprise IT and security teams struggle to implement SSL/TLS inspection policies due to a lack of compute resources and/or privacy concerns.

"As a result, encrypted channels create a significant blind spot in their security postures. Zscaler's new report on the state of encrypted attacks demonstrates that the most effective way to prevent encrypted attacks is with a scalable, cloud-based proxy architecture to inspect all encrypted traffic, which is essential to a holistic zero trust security strategy," Desai said.

The researchers found that cryptomining is becoming less prevalent as cybercriminals move toward more lucrative options like ransomware.

Zscaler noted that attacks on retailers are likely to increase during the holiday season as more companies offer digital purchase options and promote e-commerce solutions.

The company predicts a wave of malware and ransomware attacks targeting e-commerce platforms and digital payment systems between Black Friday and Christmas.

"Additionally, as the world begins its return to normal, and as businesses and public events are opening up around the globe, many employees are still working in relatively insecure environments. Getting access to critical point-of-sale systems is extremely attractive to cybercriminals as it opens the door to huge profits," the report noted.

Healthcare and governmental organizations saw a decrease in attacks but overall, seven industries saw attack rates increase from threats in SSL and TLS traffic.

Desai attributed the decrease to increased law enforcement scrutiny following the attacks on Colonial Pipeline and other critical industries. Desai noted that both healthcare and government were the most frequently targeted sectors in 2020, prompting many organizations within both industries to stiffen their security posture.

The UK, US, India, Australia and France led the way as the top five targets of encrypted attacks.

When broken down by region, Zscaler ThreatLabz researchers found that Europe saw the most attacks at more than 7.2 billion, followed by the Asia Pacific region at almost 5 billion and North America, which had about 2.8 billion. The UK led Europe with 5.4 billion encrypted attacks targeting them followed by the US and India, which both had more than 2 billion attacks sent their way.

6.EU Team Make Progress Toward European-Only Compact Quantum Computer That Could Run on Solar Power

by Matt Swayne
https://thequantumdaily.com/2021/10/28/eu-team-make-progress-toward-european-only-compact-quantum-computer-that-could-run-on-solar-power/

A team of researchers at the Institute for Experimental Physics of the University of Innsbruck, Austria, say they have built a prototype for a compact quantum computer. The team is associated with the EU Flagship Quantum Technologies.

It's so compact, the researchers are investigating whether it can be run on solar power.

According to a statement from the organization, the device is completely European.

“It is European born-and-bred. It is build with European parts and has demonstrated a world-class ability to entangle 24 qubits – a necessary condition for genuine quantum computations,” according to the statement.

It is designed to fit quantum-computing experiments into the smallest space possible.

The project to build the device is could move Europe from an over-reliance of services outside of the region.

According to the statement: “This quantum computer is available online to interested users, from individual to corporate users, through the AQT Cloud Access, and as such, it offers a competitive European alternative to the traditional big tech giants such as Google, IBM, or Alibaba. It also represents a great step forward in ensuring Europe’s technological sovereignty and reducing our dependency on foreign technology computing.”

This quantum computer design features low power consumption. It is currently estimated to use 1.5 kilowatts – or the same amount of energy needed to power a kettle. The researchers in the University of Innsbruck are exploring how to power the device using solar panels.

A range of use cases fits the device.

“All in all, this first computer with quantum acceleration could address industrial and public needs such as predicting the stability of complex molecules in chemistry for intelligent materials or vaccine development, or yet optimizing and saving energy distribution in complex grids,” the statement reads. “By offering the next generation of quantum capabilities and services in a secure, energy-efficient and sustainable manner, this quantum computer contributes directly to the objectives of the European Green Deal.”

Quantum computers could be tied to a grid of supercomputers, “forming ‘hybrid ’machines that blend the best of quantum and classical computing technologies.”

Ultimately, it’s more than a research device, according to the organization: “European industry and academia will enormously benefit, as quantum computers hold the promise to solve problems within minutes that are out of reach for today’s supercomputers because they would take millennia to solve.”

7.Researchers to Develop Cryptographic Protocol Addressing Security and Privacy Vulnerabilities in Electric Vehicles

by BW Online Bureau
http://bweducation.businessworld.in/article/Researchers-To-Develop-Cryptographic-Protocol-Addressing-Security-And-Privacy-Vulnerabilities-In-Electric-Vehicles/28-10-2021-410180/

National Institute of Technology Andhra Pradesh Researchers working with an international team have developed a protocol to address major security and privacy vulnerabilities in the dynamic charging of electric vehicles.

The Institute worked with Researchers from IIIT Hyderabad, IIIT Naya Raipur, Kyungpook National University (South Korea), and University of Wollongong (Australia), to develop this protocol.

A group of interdisciplinary researchers led by Dr Alavalapati Goutham Reddy and Prof. Ashok Kumar Das developed an **Authentication with Key Agreement Protocol** for EV Dynamic Charging Infrastructure Entities and published their findings in the reputed peer-reviewed journal IEEE Transaction on Vehicular Technology. These findings demonstrate that messages exchanged between electric vehicles and dynamic charging infrastructure are secure, preventing attackers from tracking the vehicle and gaining any benefits.

As Electric Vehicles are electric-powered, researchers have studied static, quasi-static, and dynamic charging systems. Static charging, which allows consumers to park at their homes or offices, needs the car to be immobile. It requires a connecting wire and a plug-in charger causes range anxiety and is unsafe in the wet. Quasi charging is used to charge vehicles that stop briefly, including at traffic lights or bus stops.

However, once dynamic charging is deployed in the selected areas, quasi-charging will be simple to execute. These challenges demand more investigation before global electric vehicle adoption. To address the aforementioned challenges, scientists have developed the most practical technique for charging electric vehicles on the go. ICPT is the most efficient method for charging electric vehicles while driving.

Dynamic charging allows for on-the-go charging. This eliminates the need for large-capacity batteries and lowers battery costs. Dynamic charging allows Electric Vehicles to charge while driving by burying Charging Pads (CPs) beneath the road. This saves time for drivers who no longer need to stop at charging facilities. Dynamic charging would be a new revolution and a boon to the transportation sector.

Dynamic charging is still a work in progress because it requires precise coordination between electric vehicles, highway infrastructure, and charging stations. As a result of the wide range of communication principals involved, novel technologies employed, messages sent among communicating principals, and charging infrastructure implemented in places like homes, offices, and public stations, hint at several security issues to be considered, such as message tampering, spoofing, or delaying among others to disconcert the charging service.

The designed protocol is based on elliptic curve cryptography, hash functions and chains, concatenation, and exclusive or operations, which aids in its implementation simplicity. The protocol is immune to man-in-the-middle attacks, impersonation attacks, replay attacks, and insider assaults while maintaining user anonymity and un-traceability. Also, the proposed protocol is more efficient than its counterparts in terms of computing and communication costs.

8.AWS and Caltech open Center for Quantum Computing

by Veronica Combs
https://www.techrepublic.com/article/aws-and-caltech-open-center-for-quantum-computing/

AWS announced Tuesday that the new Center for Quantum Computing at the California Institute of Technology is open and ready to take on the challenges of scale and error correction. AWS will have a team of hardware engineers, quantum theorists and software developers working to "push the boundaries of quantum R&D." Researchers and scientists will be able to make, test and operate quantum processors at the facility in addition to improving the processes for controlling quantum computers and scaling the hardware such as cryogenic cooling systems and wiring.

Oskar Painter, the John G Braun Professor of Applied Physics, Head of Quantum Hardware, and Fernando Brandao, Bren Professor of Theoretical Physics, Head of Quantum Algorithms, are the technical leads of the Center.

Nadia Carlsten, head of product at the AWS Center for Quantum Computing, wrote in a blog post that the company's quantum customers are eager to collaborate with the center and build up internal expertise with the understanding that it's still early days for the technology.

Caltech has been a leader in quantum technology since the origin of the idea. Richard Feynman was a Caltech physics professor and one of the first people to talk about the idea of quantum computing. In 19994, Caltech graduate Peter Shor developed a quantum algorithm for factoring large numbers quickly, and in 1998, Caltech professor Jeff Kimble achieved quantum teleportation by sending information from one light beam to another via entanglement.

The university collaboration will connect the commercial side of quantum computing with fundamental research going on at Caltech, according to an article from the institute announcing the opening of the center.

"If we were to just take today's ideas and go forward with them, we would create a dinosaur of a quantum computer," Painter said in the article. "We need to be closely connected and tied into these basic research efforts.”

The university sees the primary goal of AWS as creating a computer architecture that builds quantum error correction into the hardware. Painter said that researchers will address the ability to scale quantum computing by many orders of magnitude as well as figuring out what problems are best solved with the technology.

The institute reports that this is the first corporate-partnership building on the Caltech campus, and it reflects Caltech's interests in bringing fundamental science to the marketplace.

"AWS will benefit from the ideas percolating here on campus," Painter said.

The institute expects the center to support Caltech students and early career scientists via scholarships, internships and seminars.

"This will be pretty amazing for students, and AWS can tap into that talent," Painter said in the article. "Those are the future engineers and scientists who are going to build quantum computers.”

Experts in quantum-related fields will contributing to the Center's work as Amazon Scholars and Amazon Visiting Academics, including:

- Liang Jiang, University of Chicago
- Alexey Gorshkov, University of Maryland
  John Preskill, Caltech
- Gil Refael, Caltech
- Amir Safavi-Naeimi, Stanford
- Dave Schuster, University of Chicago
- James Whitfield, Dartmouth

These researchers will continue to teach and conduct research at their universities while working with the Center.

9.Two Chinese teams claim to have reached primacy with quantum computers

by Bob Yirka
https://phys.org/news/2021-10-chinese-teams-primacy-quantum.html

Two teams in China are claiming that they have reached primacy with their individual quantum computers. Both have published the details of their work in the journal *Physical Review Letters*.

In the computer world, quantum primacy is the performance of calculations that are not feasible on conventional computers — others use the term "quantum advantage."

Over the past several years, several teams working with quantum computers have claimed to have reached primacy, but thus far have been met with skepticism due to questions about whether the algorithm used was the best choice possible, including the one used by Google. In this new effort, both teams are claiming that their computers leave no room for doubt.

Both of the teams in these new efforts were working at the Hefei National Laboratory for Physical Sciences at the University of Science and Technology of China, and both were led by physicist Jian-Wei Pan, who has become well known for his work with quantum entanglement.

In both efforts, the goal was to build a quantum computer capable of calculating the output probabilities of quantum circuits—a task that is relatively simple for a conventional computer to perform when there are just a few inputs and outputs. It grows increasingly difficult as the numbers rise until it becomes unfeasible.

In the first effort, the researchers used a photonic approach in building their computer. To tackle the problem of estimating output probabilities, the team used Gaussian boson sampling as a way to analyze the output. In this case, output from a 144-mode interferometer. Under this scenario, there could be 10^43 possible outcomes. The researchers claim their machine was capable of sampling the output 10^23 times as fast as a supercomputer, which, they further claim, shows quantum primacy.

The second effort involved creating a superconductor-based computer that was capable of calculating using 66 qubits — only 56 of them were used, however. Still, the researchers found the machine capable of estimating sample calculations up to 1000 times as fast as the best supercomputers, which, they claim, shows that they achieved primacy.

10.Post-quantum cryptography oversight lacking for agencies

by Dave Nyczepir
https://www.fedscoop.com/post-quantum-cryptography-oversight/

The Department of Homeland Security’s post-quantum cryptography roadmap lacks deadlines and oversight needed to ensure agencies ’compliance, according to the leader of Thales ’encryption team.

Agencies should be given a drop-dead date to submit plans for protecting their most sensitive data and modernizing their cryptographic systems to a leadership council that has yet to be designated, said Todd Moore, senior vice president of encryption products.

DHS partnered with the National Institute of Standards and Technology to develop the roadmap — intended to prepare agencies for advances in quantum computing that will break the asymmetric encryption many use to protect data and systems — but a means of enforcement is lacking.

“I think the government could do a little bit more to add weight above just the guidance,” Moore told FedScoop. “Have some sort of a way where agencies have to comply, versus maybe comply.”

The guidance does an “excellent” job of generating a sense of urgency among agencies concerning the demise of current cryptography, which is anywhere from five to 10 years off, Moore said. That sense of urgency has been building for some time with Thales seeing an uptick in inquiries from agencies, as well as the health-care and finance sectors.

DHS’s roadmap suggests agencies analyze their organizations, inventory their most sensitive data and begin taking steps to protect it today because nation-states like China are stealing that data and archiving it for later, when they have a quantum computer capable of decryption.

Current guidance falls short in this regard as well.

“It’s really understanding where that data flows, not just within one organization, but across multiple organizations,” Moore said. “I think it’s important when you map to understand those different interactions between different agencies.”

Next-generation, quantum-resistant algorithms already exist. NIST’s Post-Quantum Cryptography Standardization Process has spent the last three years evaluating them, narrowed down to seven finalists, for recommended use in the post-quantum era.

Thales sponsored one such algorithm, and only one or two will be chosen by NIST next year to be the standard — likely for digital signature and public-key encryption respectively.

Once NIST sets the standard, agencies will be able to start deploying technologies using the appropriate algorithm or algorithms, but DHS’s roadmap makes no mention of the fact agencies can and should test them out in non-production environments now, Moore said.

Thales is already modeling the algorithms so agencies and banks can look at latency and performance to see how it impacts their environments for preparedness.

“Our hardware security module for data at rest and our high-speed encryptors, which is data in motion, were able to actually insert those algorithms,” Moore said. “We call it cryptographic agility, the ability to model these post-quantum algorithms in these products.”

11. Algorithms and Accessibility: Updates from the Advanced Quantum Testbed (AQT)

by Kenna Castleberry
https://thequantumdaily.com/2021/10/25/algorithms-and-accessibility-updates-from-the-advanced-quantum-testbed-aqt/

In October of 2021, University of California, Berkeley Professor and Director Dr. Irfan Siddiqi of theAdvanced Quantum Testbed (AQT) at Lawrence Berkeley National Laboratory (Berkeley Lab) discussed the latest research in quantum computing. Given in a "fireside chat" format, Dr. Siddiqi addressed the industry and trade press, focusing on issues ranging from laboratory benchmarks to accessibility of this emerging technology.

The AQT began in 2018 as a collaborative research program funded by the Department of Energy (DOE) at Berkeley Lab to focus on advancing quantum computing. The program focuses specifically on superconducting circuits and quantum algorithms, using a multidisciplinary approach to designing and testing the technology. The AQT has been able to publish literature on successful noise control algorithms, and other algorithms for multi-qubit and qutrit processors.

In speaking at the fireside chat, Dr. Siddiqi said: "We are at a crossroads for quantum technology." He further explained the current solutions for the problems in quantum computing were not fundamental in nature, making the solutions more complex to study. The current research has shown some: "proof of principle within the experiment," according to Siddiqi, but there needs to be better alignment of the resources in order to make for more efficient research. When asked about current expectations of AQT, Siddiqi responded that the testbed was designed to engage with users on meaningful questions within quantum computing. These expectations have been transposed on several AQT projects, including the recent work with the Quantum Imaginary Time Evolution (QITE) algorithm. Using this algorithm, Siddiqi and his team were able to improve the stability of the algorithm, reaching "the ground state in energy and fidelity with a precision below 1%." This success showed the AQT what their team could do in advancing quantum computing technology.

While QITE is not a classical-quantum hybrid algorithm, Siddiqi referenced it as an inspiration for these hybrid algorithms that many businesses could end up adopting. In looking at these hybrids, Siddiqi emphasized that the quantum component is utilized to help overcome classical computing issues. These hybrids also require different forms of evaluation to determine how successful the algorithms are.

Accessibility and Diversity:

While AQT looks at ways to advance quantum computing, it also focuses on the accessibility of the technology. In explaining how the program is working toward making the hardware more cost-effective, Siddiqi mentioned that the testbed was free to users. Additionally, the AQT works at bringing in researchers of all ages and backgrounds. "We are not monolithic. There is diversity in terms of approaches, there's diversity in terms of hardware, there's diversity in terms of intellectual capital and ideas, and then there's diversity in terms of human capital." Siddiqi said. He added that high school students and undergraduates are often accepted into the AQT program as they sometimes give the best ideas. AQT reflects the broader science mission at a DOE-funded laboratory by partnering with community colleges, as well as state boards and local governments. “Quantum technology reaches many,” stated Siddiqi. “This is a very interesting revolution in the technological sector and that’s really an opportunity to expand beyond some very narrow definition of what quantum computing is. The technology is definitely broader and will evolve, so we have actually an opportunity to have a broader conversation with a broader group of folks about what this field should be. And I think the output will be much better that way.” He went on to explain that AQT is also working to develop quantum engineering as a discipline, so more individuals can study it and pursue a successful career in the quantum science sector.

One of the researchers at the fireside chat, Ravi Naik, AQT’s measurement lead, mentioned how grateful he was for Siddiqi’s work. Naik originally joined Siddiqi’s research group at UC Berkeley as an undergraduate, before leaving for other endeavors and later returning as a postdoc and later becoming a career-track research scientist at Berkeley Lab. “I’m grateful for the time I’ve had to work with the testbed and its users,” Naik exclaimed. “I’m so thrilled to see how many people are involved across the world, and how much the field has grown.”

12.U.S. GAO Releases Report on Risks and Rewards of Quantum Computing and Communications

by Matt Swayne
https://thequantumdaily.com/2021/10/24/u-s-gao-releases-report-on-risks-and-rewards-of-quantum-computing-and-communications/

The U.S. Government Accountability Office offers a Spaghetti Western assessment of the future of quantum computing — offering critical factors that need to be addressed to enhance the good, mitigate the bad and even beautify a little of the ugly in the emerging industry.

The office released its assessment of quantum computing recently, acknowledging the transformative power of quantum computing and communication technologies.

According to the report: “Future quantum computers could have high-value applications in security, cryptography, drug development, and energy. Future quantum communications could allow for secure communications by making information challenging to intercept without the eavesdropper being detected.”

The office sees the considerable progress of quantum computing and communications technology. However, the officials also see quantum computing impact will likely take a decade and billions of dollars for the technology to fully emerge.

The GAO identified four factors that will affect quantum technology development and use: collaboration, workforce size and skill, investment and the supply chain. These four factors are likely no surprise to the global quantum ecosystem — and, likely, they are among the stakeholders who pointed out both the positive potential and potential problems.

Collaboration

Recently, members of the quantum community have identified government interference with collaboration as a major block. The GAO recognizes “Export controls may complicate international collaboration, but are also needed to manage national security risks.”

Workforce Development

The report offers recommendations on quantum workforce development, specifically: “Policymakers could consider ways to expand the quantum technology workforce by, for example: Leveraging existing programs and creating new ones Promoting job training Facilitating appropriate hiring of an international workforce who are deemed not to pose a national security risk.”

Investment

While billions are flowing into quantum computing and communication from private markets, the GAO suggests it might not be enough and further government funding is suggested.

They recommend:“ Policymakers could consider ways to incentivize or support investment in quantum technology development, such as investments targeted toward specific results; continued investment in quantum technology research centers and grand challenges to spur solutions from the public.”

Supply Chain

Finally, the quantum supply chain is recognized as incredible complex and vulnerable. GAO experts and stakeholders recommend the following steps to establish, secure and optimize the supply chain by: “Enhancing efforts to identify gaps in the global supply chain and expanding fabrication capabilities for items with an at-risk supply chain.”

According to the office, the assessment was derived from key reports and scientific literature; interviewed government, industry, academic representatives, and potential end users; and convened a meeting of experts in collaboration with the National Academies of Sciences, Engineering, and Medicine.

13. Scientists achieved quantum communication over fiber more than 600 kilometers long

by AMIT MALEWAR
https://www.techexplorist.com/scientists-achieved-quantum-communication-over-fiber-600-kilometers-long/41951/

A new study extends the range of fiber-based quantum communications beyond 600km for the first time. Scientists implemented a new signal stabilization technique and used the twin-field quantum key distribution (QKD) protocol.

Mirko Pittaluga from Toshiba Europe Limited and the University of Leeds said, "This will allow us to build national and continental scale fiber networks connecting major metropolitan areas. Together with satellite links, we can now envisage truly global quantum networks."

Quantum key distribution allows two people in different places to establish a common secret string of bits by exchanging photons typically transmitted over an optical fiber. Achieving transmission over long distances has a fundamental limit to how far the photons can travel before the signal degrades due to scattering or absorption.

Optical repeaters solve this problem for traditional fiber optic data transmission; however, creating a reliable repeater for quantum encoded information is challenging.

The newly developed twin-field QKD protocol has potentially overcome the distance limitation, but it requires fibers to be used over long distances.

In this study, scientists created an experimental setup and phase stabilization technique for twin-field QKD. The stabilization approach, based on wavelength division multiplexing, uses two optical reference signals at different wavelengths to minimize the phase fluctuations over long distances.

Scientists demonstrated that the new approach could accomplish repeater-like performance while tolerating optical losses beyond the traditional limit of 100 dB over a 605-kilometer-long quantum channel. They were also able to test different variants of the TF-QKD protocol. The new stabilization approach could also be applied to other quantum communication protocols and applications, such as improving interferometric telescopes.

These results were obtained in a laboratory environment, but recently obtained experimental evidence confirms the applicability of this stabilization technique on field-deployed fibers. The team is now working to perform a field trial test.

Mirko Pittaluga from Toshiba Europe Limited and the University of Leeds, both in the UK, will present the research at the Frontiers in Optics + Laser Science Conference (FiO LS) all-virtual meeting, 01 – 04 November 2021.

14.ISARA, Carillon and Crypto4A Partnership enables a world first Canadian fully integrated Quantum-Safe Now PKI solution

by Crypto4A
https://www.newswire.ca/news-releases/isara-carillon-and-crypto4a-partnership-enables-a-world-first-canadian-fully-integrated-quantum-safe-now-pki-solution-882977605.html?utm_medium=email&_hsmi=174804691&_hsenc=p2ANqtz-_BFCw3wc8tFp1Pgzwh_Y3-TBfcTFae5jwk_pDLcnVSEE-R9TAE-qscU-ouyZA8EgQRleZPlgwouOA7-SYBsQ4jU7uDing&utm_content=174804691&utm_source=hs_email

Crypto4A Technologies Inc., ISARA Corp., and Carillon Information Security Inc. today announced their partnership agreement focused on providing organizations with a next generation Quantum Safe NowTM Public Key Infrastructure (PKI) solution.

The Quantum-Safe Now™ PKI solution integrates ISARA's Radiate Quantum-safe Toolkit and Catalyst Agile Digital Certificate Methodology, which provide hybrid crypto-agility, with Carillon's world class PKI CertServ ID Management Suite operating on Crypto4A's QxEDGE™ and QxCloud™ Hybrid Security Platform (HSP).

By working together, the three Canadian organizations provide a world first quantum safe PKI solution running on purpose-built hybrid crypto-agile hardware.

As part of the partnership, the companies intend to develop and market seamless, easy to use quantum-safe PKI cryptographic solutions that ease digital transformations, enable cryptographic agility and simplify cryptographic management.

Today's connected economies, identity based digital transformations, DevSecOps teams and cloud-based deployments require new cryptographic capabilities based on quantum-safe software and hardware to provide enterprises with the forward agility, seamless access, security and controls required for cloud, edge, and end user environments.

"ISARA's suite of proven crypto-agile capabilities effectively complements the proven capabilities of both Carillon's PKI software and Crypto4A's hardware based crypto-agility resulting in a more robust and easier to use Quantum-Safe Now™ PKI solution. Our approach is to enable customers to discover and manage their cryptographic capabilities in an agile, quantum-safe and trusted way. Our collective experiences, knowledge and integrated Quantum Safe Now™ PKI solution de-risks digital transformations and migrations to address the evolving security requirements for today and tomorrow," said Scott Totzke, CEO and Co-founder at ISARA.

"Identity based digital environments, applications and relationships rely on cryptography for their trust, innovation, security and privacy. By working with ISARA and Carillon, we demonstrate the power of the Canadian cryptography industry to elevate the original PKI architecture as well as demonstrate the agile capabilities of our FPGA based QxTrust Architecture™(QxTA™). As progress is made in better cloud and edge security, privacy and data management, new requirements are emerging that place material stress on the foundations of today's cryptographic hardware. This new collaborative offering helps to remove some of these stresses and represents our approach to cooperation", said John Scott, CEO of Crypto4A.

"We are excited to be partnering with Crypto4A and ISARA on this common PKI initiative. The experience that they both bring from a cryptography and an engineering perspective, provides Carillon and its customers with an integrated approach to an agile Quantum Safe Now™ PKI solution. Quantum Safe Now™ demonstrates our ongoing commitment to meet the emerging needs of the connected enterprise for innovation with digital trust", said Patrick Patterson, President and Chief PKI Architect of Carillon.

15.Gartner advises tech leaders to prepare for action as quantum computing spreads

by Jack Vaughan
https://venturebeat.com/2021/10/21/gartner-advises-tech-leaders-to-prepare-for-action-as-quantum-computing-spreads/

Quantum computing has hit the radar of technical leaders, because of the huge efficiency it offers at scale. It will take years to develop for most applications, however, even as it makes limited progress in the near term in highly specialized fields of materials science and cryptography.

Quantum methods are gaining more rapid attention, however, with special tools for AI, as seen in recent developments around natural language processing that could open up the “black box” of today’s neural networks.

Last week’s release of a Quantum Natural Language Processing (QNLP) toolkit by Cambridge Quantum shows the new possibilities.

Known as lambeq, the kit takes the form of a conventional Python repository that is hosted on GitHub. It follows the arrival at Cambridge Quantum of noted AI and NLP researchers and affords the chance for hands-on experience in QNLP.

The lambeq package, which takes its name from late semantics researcher Joachim Lambek, is said to convert sentences into quantum circuits, offering a new view into text mining, language translation, and bioinformatics corpora.

Using quantum principles, NLP can provide explainability not possible in “bag of words” neural approaches done on classical computers today, according to Bob Coecke, the chief scientist at Cambridge Quantum. QNLP, he said, layers a compositional structure on circuits. As represented on schema, these structures do not look too unlike parsed sentences on grade-school blackboards.

Presently popular methods of NLP “don’t have an ability to compose things together to find a meaning,” Coecke told VentureBeat. “What we want to bring in is compositionality in the classical sense — to use the same compositional structure. We want to bring reasoning back.”

Cambridge Quantum's efforts to expand quantum infrastructure got significant backing earlier this year when Honeywell said it would merge its own quantum computing operations with Cambridge Quantum, to form an independent company to pursue cybersecurity, drug discovery, optimization, material science, and other applications, including AI.

Honeywell said it would invest between $270 million – $300 million in the new operation. Cambridge Quantum said it would remain independent, working with various quantum computing players, including IBM.

The lambeq work is part of an overall AI project that is the longest-term project among the efforts at Cambridge Quantum, said Ilyas Khan, founder, and CEO of Cambridge Quantum, in an e-mail interview.

"We might be pleasantly surprised in terms of timelines, but we believe that NLP is right at the heart of AI more generally and therefore something that will really come to the fore as quantum computers scale," he said. Khan cited cybersecurity and quantum chemistry as the most advanced application areas in Cambridge Quantum's estimation.

What kind of timeline does Khan see ahead for quantum hardware?

"There is a very well-informed consensus not only about the hardware roadmap," he replied, citing Honeywell and IBM among credible corporate players in this regard.

These "and the very well amplified statement by Google about having fault-tolerant computers by 2029 are just some of the reasons why we say that the timelines are generally well-understood," Khan said.

The march of quantum

Alliances, modeling advances, mergers, and even — in the cases of IonQ and Rigetti — public offerings comprise most of the quantum computing industry advancements of late. Often hybrid couplings of quantum and classical computing features are involved.

New developments in the quantum industry include:

- D-Wave, builders of a quantum annealing computer that carried forward much of the early research in the area, this year added constrained quadratic model solvers to hybrid tooling for problems that run across classical and quantum systems;
- Rigetti Computing is working with Riverlane and Astex Pharmaceuticals to pair Rigetti's quantum processors with cloud-based classical computing resources that, in effect, test quantum algorithms for drug discovery on a hybrid platform that mixes classical and quantum processing;
- IBM said it would partner with European electric utility company E.ON to develop workflow solutions for future decentralized electrical grids using the open-source Qiskit quantum computing SDK and the IBM Cloud; and,
- Sandbox, at Alphabet, has reportedly launched APIs that let developers use Google Tensor Processing Units to simulate quantum computing workloads.

Use case drill down

Indications are that, as researchers bounce between breakthroughs and setbacks, a variety of new quantum-inspired algorithms and software tools will appear. Enterprises need to pick targets carefully while treading some novel ground.

Gartner analyst Chirag Dekate emphasized that, where applicable, enterprises should begin to prepare for quantum computing. He spoke this week at Gartner IT Symposium/Xpo 2021 Americas.

He said companies should be sure not to outsource quantum innovation, but to instead use this opportunity to foster skills via small quantum working groups.

“Starting early is the surest form of success,” he said.

He said enterprise decision-makers must drill down on very specific use cases, as they prepare for quantum commercialization.

“Quantum computing is not a general-purpose technology — we cannot use quantum computing to address all the business problems that we currently experience,” Dekate told the assembled and virtual conference audiences.

Gartner’s Hype Cycle for Computing Infrastructure for 2021 has it that more than 10 years will elapse before quantum computing reaches the Plateau of Productivity. That’s the place where the analyst firm expects IT users to truly benefit from employing a given technology.

The assessment is the same as it was in 2020, as is quantum computing’s present post on the Peak of Inflated Expectations — Gartner’s designation for rising technologies that are considered overhyped.

16.Toshiba Shrinks Quantum Key Distribution Technology to a Semiconductor Chip

by Daniel Migdal
https://news.toshiba.com/press-releases/press-release-details/2021/Toshiba-Shrinks-Quantum-Key-Distribution-Technology-to-a-Semiconductor-Chip/default.aspx

Toshiba Europe Ltd today (21 Oct 2021) announced it has developed the world’s first chip-based quantum key distribution (QKD) system. This advance will enable the mass manufacture of quantum security technology, bringing its application to a much wider range of scenarios including to Internet of Things (IoT) solutions.

QKD addresses the demand for cryptography which will remain secure from attack by the supercomputers of tomorrow. In particular, a large-scale quantum computer will be able to efficiently solve the difficult mathematical problems that are the basis of the public key cryptography widely used today for secure communications and e-commerce. In contrast, the protocols used for quantum cryptography can be proven secure from first principles and will not be vulnerable to attack by a quantum computer, or indeed any computer in the future.

The QKD market is expected to grow to approximately $20 billion worldwide in FY20351. Large quantum-secured fibre networks are currently under construction in Europe and South-East Asia, and there are plans to launch satellites that can extend the networks to a global scale. In October 2020, Toshiba released two products for fibre-based QKD, which are based on discrete optical components. Together with project partners, Toshiba has implemented quantum-secured metro networks and long-distance fibre optic backbone links in the UK, Europe, US and Japan.

Manufacturing advances

For quantum cryptography to become as ubiquitous as the algorithmic cryptography we use today, it is important that the size, weight and power consumption are further reduced. This is especially true for extending QKD and quantum random number generators (QRNG) into new domains such as the last-mile connection to the customer or IoT. The development of chip-based solutions is essential to enabling mass market applications, which will be integral to the realisation of a quantum-ready economy.

Toshiba has developed techniques for shrinking the optical circuits used for QKD and QRNG into tiny semiconductor chips. These are not only much smaller and lighter than their fibre optic counterparts, but also consume less power. Most significantly, many can be fabricated in parallel on the same semiconductor wafer using standard techniques used within the semiconductor industry, allowing them to be manufactured in much larger numbers. For example, the quantum transmitter chips developed by Toshiba measure just 2x6mm, allowing several hundred chips to be produced simultaneously on a wafer.

Andrew Shields, Head of Quantum Technology at Toshiba Europe, remarked, “Photonic integration will allow us to manufacture quantum security devices in volume in a highly repeatable fashion. It will enable the production of quantum products in a smaller form factor, and subsequently allow the roll out of QKD into a larger fraction of the telecom and datacom network.”

Taro Shimada, Corporate Senior Vice President and Chief Digital Officer of Toshiba Corporation comments, “Toshiba has invested in quantum technology R&D in the UK for over two decades. This latest advancement is highly significant, as it will allow us to manufacture and deliver QKD in much larger quantities. It is an important milestone towards our vision of building a platform for quantum-safe communications based upon ubiquitous quantum security devices.”

Part of this work was funded by the Innovate UK Collaborative R&D Project AQuaSeC, through the Industrial Strategy Challenge Fund. The details of the advancement are published in the scientific journal, Nature Photonics.

Technical Summary

QKD systems typically comprise a complex fibre-optic circuit, integrating discrete components, such as lasers, electro-optic modulators, beam-splitters and fibre couplers. As these components are relatively bulky and expensive, the purpose of this work was to develop a QKD system in which the fibre-optic circuit and devices are written in millimetre scale semiconductor chips.

Toshiba has developed the first complete QKD prototype in which quantum photonic chips of different functionality are deployed. Random bits for preparing and measuring the qubits are produced in quantum random number generator (QRNG) chips and converted in real-time into high-speed modulation patterns for the chip-based QKD transmitter (QTx) and receiver (QRx) using field-programmable gate arrays (FPGAs). Photons are detected using fast-gated single photon detectors. Sifting, photon statistics evaluation, time synchronisation and phase stabilisation are done via a 10 Gb/s optical link between the FPGA cores, enabling autonomous operation over extended periods of time. As part of the demonstration, the chip QKD system was interfaced with a commercial encryptor, allowing secure data transfer with a bit rate up to 100 Gb/s.

To promote integration into conventional communication infrastructures, the QKD units are assembled in compact 1U rackmount cases. The QRx and QTx chips are packaged into C-form-factor-pluggable-2 (CFP2) modules, a widespread form-factor in coherent optical communications, to ensure forward compatibility of the system with successive QKD chip generations, making it easily upgradeable. Off-the-shelf 10 Gb/s small-form-factor pluggable (SFP) modules are used for the public communication channels.

Taofiq Paraiso, lead author of the Nature Photonics paper describing the chip-scale QKD system, says: "We are witnessing with photonic integrated circuits a similar revolution to that which occurred with electronic circuits. PICs are continuously serving more and more diverse applications. Of course, the requirements for quantum PICs are more stringent than for conventional applications, but this work shows that a fully deployable chip-based QKD system is now attainable, marking the end of an important challenge for quantum technologies. This opens a wide-range of perspectives for the deployment of compact, plug-and-play quantum devices that will certainly strongly impact our society."

17.Edward Snowden warns weakening encryption would have dire consequences: 'Privacy is power'

by Ryan Browne
https://www.cnbc.com/2021/10/22/edward-snowden-warns-weakening-encryption-would-be-colossal-mistake.html

Undermining encryption systems to give governments access to people's personal messages would be a "colossal mistake" with fatal consequences, former U.S. whistleblower Edward Snowden has warned.

"Privacy is power," said Snowden, speaking from Russia via video link at a press conference Thursday marking the first "Global Encryption Day."

It comes as governments around the world pile pressure on tech giants like Facebook and Apple to grant authorities access to encrypted messages. Several countries are calling for so-called "backdoors" which would allow them to bypass encryption.

The U.S., European Union, Australia, Russia and China are among the jurisdictions "trying to develop means and methods for requiring weak encryption systems," Snowden claimed.

Tech firms argue that end-to-end encryption, which scrambles messages during delivery so that they can only be viewed by the intended recipient, is important for ensuring users 'privacy.

But governments are concerned about the technology preventing law enforcement from investigating severe crimes like terrorism and child sexual abuse.

The use of end-to-end encryption has long been a point of contention between governments and large tech companies. Apple, for example, has frequently clashed with U.S. authorities over encryption and data privacy.

Privacy “was meant to be the individuals ’power,” Snowden continued. “It was meant to protect us, to shelter us from the institutional behemoths that sort of marched in the cities of our day, whether it’s the modern time or the time before.”

“It was an insulating layer that allowed those of us who wield very little power in society, because we are individuals, to think and act and associate freely,” he added.

The former intelligence consultant in 2013 leaked classified documents to journalists describing surveillance programs run by the NSA to tap people’s cell phones and internet communications. To some, he is viewed as a hero; to others, a traitor to his country.

Facebook ‘doesn’t care’

Calling out Facebook and other tech giants, Snowden said: “The same companies that have worked so hard to spread encryption over the years are now beginning to fear the next step.”

“Groups like Facebook want to have as much information as possible. So now they’re limiting where they’ll use end-to-end encryption. They’ll say, for things that we don’t want to have a business liability for, we’ll adopt end-to-end encryption.”

“They’re not socially minded,” Snowden added. “They don’t care. They care about their interests.”

Facebook was not immediately available for comment when contacted by CNBC.

His comments appeared to contradict Facebook’s pro-encryption messaging. The company has faced a backlash from officials in the U.S. and Britain over plans to bring end-to-end encryption to all its messaging apps.

Last year, the U.S. and its “Five Eyes” allies — the U.K., Canada, Australia and New Zealand — released a statement calling on tech companies to develop a solution that enables law enforcement to access tightly encrypted messages.

Meanwhile, the European Union is pushing the tech industry to look for ways to provide law enforcement with access to digital evidence “without prohibiting or weakening encryption.”

Apple recently delayed plans to check users ’devices for images of child sexual exploitation after criticisms from privacy advocates.

According to Apple, the system wouldn’t actually scan people’s photos but instead search for digital “fingerprints” that match with a U.S. database of child abuse material. However, the Electronic Frontier Foundation slammed the move as a “backdoor” for government snooping.

18. IDQ unveils Cerberis XGR QKD Platform

by Julien Levallois

https://www.swissquantumhub.com/idq-unveils-cerberis-xgr-qkd-platform/

ID Quantique (IDQ), the world leader in quantum cybersecurity, today launched the Cerberis XGR, an open QKD platform designed as a versatile research tool for academic and technology evaluation labs wanting to test the technology, run QKD testbeds or build a quantum lab.

Safety of current encryption methods, and especially of the key exchange mechanisms based on asymmetric cryptography, is a major concern today particularly for governments and enterprises which must protect data for five to ten years or more. Possible back-doors in current systems combined with massive computing power already put high-value sensitive data at risk of being decrypted by malevolent actors. Moreover, the arrival of quantum computers will render asymmetric key exchanges unsafe: encrypted data can be stored now and easily decrypted later.

Quantum Key Distribution (QKD) enables unbreakable communications and future-proof data privacy. It is the only known cryptographic technique which provides proven secrecy of encryption keys, as well as long-term data confidentiality and integrity. ID Quantique has been helping companies to get started with Quantum Cyber Security for 20 years. Since 2007, it has commercialized QKD systems to governments, enterprises, and industrial customers in more than 60 countries and on every continent.

Recently, IDQ launched its 4th generation of QKD Systems, the XG series. The Cerberis XGR is the second model in the series.

This open QKD platform is designed for academia, research institutes and innovation labs wanting to evaluate and test the technology.

Users can experiment different parameter set-up and configurations, in both automated and manual modes. Its user-friendly interface and comprehensive software suite with full real-time monitoring and management system enables to easily familiarize oneself with this technology and gain knowledge.

ID Quantique also offers on-demand services such as tailored training, product customization or quantum risk assessment to best fit its users 'needs.

> *The study of QKD has acquired a new sense of urgency: it is simply not possible to wait until the arrival of quantum computers to design and test suitable cryptographic methods. The Cerberis XGR will help teams get started with QKD and evaluate how it fits into networks. Its design and associated services are made to help any organization get started now and lead quantum innovation in their respective field.*

Grégoire Ribordy, CEO and co-founder of ID Quantique

19.NIST seeks industry help to smooth transition to quantum-resistant encryption

by Derek B. Johnson

https://www.scmagazine.com/analysis/encryption/nist-seeks-industry-help-to-smooth-transition-to-quantum-resistant-encryption

Government agencies and the private sector have been patiently waiting for the National Institute of Standards and Technology to approve its new "post-quantum" cryptographic algorithms so they can begin the long, arduous process of switching out their classical encryption for new protocols that can better protect against future quantum codebreaking.

But for years, waiting is all these entities could do, as NIST doesn't expect to formally bless new algorithms for another 1-2 years. Now, the agency is explicitly asking for companies and research firms to apply for cooperative research partnerships with the government to help develop technology and tools that would inform a "roadmap" the agency is devising to guide businesses and agencies on implementation.

Organizations can apply for Cooperative Research and Development Agreements with NIST, where they will work to develop or offer proofs of concept for tools that help integrators, customers and developers of products that use public key encryption identify the devices and systems that are most in need up updates.

"To meet the need to accelerate migration to quantum-resistant cryptography, the [National Cybersecurity Center of Excellence] Migration to Post-Quantum Cryptography project will demonstrate tools for discovery of quantum-vulnerable cryptographic code or dependencies on such code," the agency announced in a Federal Register notice set to publish tomorrow. "The tools to be demonstrated provide automation assistance in identifying where and how public-key cryptography is being used in data centers on-premises or in the cloud and distributed compute, storage, and network infrastructures."

The partnership will explore tooling options across a wide variety of technologies and components that rely on strong encryption, including hardware, software and operating systems, network infrastructure, assets and endpoints and others. The selected organizations contributions will include "establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities."

Organizations have a month to submit letters of interest, but the agency notes that it will commence the work "as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities."

For years, the cybersecurity community has known that this transition is coming, but right now many organizations are between a rock and a hard place: eager to move forward with the years-long process of switching out encryption protocols as soon as possible but unable to do so until NIST finishes approving its algorithms.

The National Security Agency is one of the few agencies or organizations with the mission, budget and cryptography skills to press ahead before waiting for NIST to finish its project, though it intends to select a lattice-based algorithm from among the NIST finalists to underpin its future encryption. The agency also put out guidance to the public on a range of classical, symmetric encryption options in the interim that they believe are resilient against hypothetical quantum code breaking techniques.

It should be pointed out that the NSA has a well-known surveillance mission and a history and record around mucking with NIST encryption standards that leave some understandably reluctant to rely on them as an authority.

But they're also one of the few organizations in the world with the cryptography expertise to chart their own path and are largely in the same boat as everyone else, needing to move away from the classical encryption options they've relied on for decades but dealing with loads of uncertainty around how best to do it. Additionally, intelligence agencies like NSA have a much bigger target on their back compared to almost every other organization on the planet and must protect their data from well-resourced foreign intelligence agencies and Advanced Persistent Threat hacking groups.

That gives them plenty of incentive to move faster.

“We’re looking at the post-quantum computer era, how we make sure that we’re there before the quantum computers are,” said NSA Cybersecurity Director Rob Joyce this month. “That’s a really important thing for our national security systems, where we want to keep secrets for decades, right? So we’ve got to be rolling out that post-quantum capability today to secure today’s secrets for decades into the future.”

While technically those algorithms would only be mandatory for government agencies and contractors, NIST’s technology and cybersecurity standards are widely used as benchmarks for the private sector and other standards organizations, meaning the algorithms they select will likely become the dominant market options in a post-quantum landscape.Those that move ahead now risk selecting unapproved algorithms or vendor products that may make not make NIST’s final cut, while continuing to wait leaves them exposed to potential data harvesting attacks from foreign governments and Advanced Persistent Threat espionage groups or pushes out their timeline for completion even further back.

Dustin Moody, a mathematician for NIST and manager of its post-quantum cryptography project, explained to SC Media earlier this year what organizations are risking by moving too quickly.

“By purchasing and implementing early, you risk using algorithms that are not the ones that end up being standardized. You risk not being interoperable with those that will use the standard,” Moody told SC Media. “Although there is always a security risk that a cryptographic algorithm may be broken [or] attacked, the risk is higher using algorithms that have not been standardized - particularly in this field of post-quantum cryptography. Throughout our [project] we have seen algorithms broken in each round of our process.”

20.IBM and Raytheon Technologies collaborate on AI, cryptography and quantum technologies

https://www.scientific-computing.com/news/ibm-and-raytheon-technologies-collaborate-ai-cryptography-and-quantum-technologies

IBM and Raytheon Technologies have announced a collaboration to jointly develop advanced artificial intelligence (AI), cryptographic and quantum solutions for the aerospace, defence and intelligence industries, including the federal government, as part of a strategic collaboration agreement.

Artificial intelligence and quantum technologies give aerospace and government customers the ability to design systems more quickly, better secure their communications networks and improve decision-making processes. By combining IBM's breakthrough commercial research with Raytheon Technologies' own research, plus aerospace and defence expertise, the companies will be able to crack once-unsolvable challenges.

Dario Gil, senior vice president, IBM, and director of research comments: ‘The rapid advancement of quantum computing and its exponential capabilities has spawned one of the greatest technological races in recent history – one that demands unprecedented agility and speed. Our new collaboration with Raytheon Technologies will be a catalyst in advancing these state-of-the-art technologies – combining their expertise in aerospace, defence and intelligence with IBM's next-generation technologies to make discovery faster, and the scope of that discovery larger than ever.’

In addition to artificial intelligence and quantum, the companies will jointly research and develop advanced cryptographic technologies that lie at the heart of some of the toughest problems faced by the aerospace industry and government agencies.

Mark Russell, Raytheon Technologies chief technology officer added: ‘Take something as fundamental as encrypted communications. As computing and quantum technologies advance, existing cybersecurity and cryptography methods are at risk of becoming vulnerable. IBM and Raytheon Technologies will now be able to collaboratively help customers maintain secure communications and defend their networks better than previously possible.’

The companies are building a technical collaboration team to quickly insert IBM's commercial technologies into active aerospace, defence and intelligence programs. The same team will also identify promising technologies for jointly developing long-term system solutions by investing research dollars and talent.

21.Castle Shield Holdings, LLC Adds Post-Quantum Cryptography (PQC) to Its Data-in-Motion VPN Solution

by Milton Mattox
https://www.businesswire.com/news/home/20211011005150/en/Castle-Shield-Holdings-LLC-Adds-Post-Quantum-Cryptography-PQC-to-Its-Data-in-Motion-VPN-Solution

Castle Shield Holdings, LLC., has successfully integrated post-quantum cryptography (PQC) into its Aeolus VPN enterprise data-in-motion solution. Aeolus VPN now offers point-to-point asymmetric PQC and symmetric encryption for UDP and TCP on Windows, Linux and macOS platforms. Aeolus VPN offers a streamlined approach to privacy which results in more stability and lower latency that is a perfect addition to enterprise data-in-motion security for both classic and post-quantum computing environments.

In April, Castle Shield released Aeolus VPN which protects data between two or more network points. Please refer to our press release dated April 19, 2021, for additional product specification.

Post-Quantum Cryptography

PQC refers to a set of classical cryptographic asymmetric algorithms that are believed to be “quantum-safe,” meaning that they are expected to remain safe even in the presence of quantum computers. The National Institute of Standards and Technology (NIST) has narrowed down the original 69 submissions to 7 finalists and 8 alternate candidates. Castle Shield has integrated two of the NIST Round 3 finalists PQC asymmetric encryption. NIST will select a small subset of these algorithms that will form the core of the first post-quantum cryptography standards. Selected candidates from both the finalist and alternate groups will be announced in 2022 and 2024 respectively. NIST's objective with PQC is to offer a secure mechanism for exchanging encryption keys that cannot be broken by quantum computers.

Why is Implementing PQC Important Today?

Many applications today are protected by asymmetric encryption key exchange protocols known as "public key cryptography" or PKC. Examples include RSA, RSA-EC, DSA, DH, and ECDH. These protocols rely on the assumption that it would take today's most powerful classical computers thousands of years to solve certain mathematical problems (e.g., factoring large numbers or computing a discrete logarithm).

Quantum computers are expected to break these cryptographic schemes in short order. If quantum computers were widely available today, most, if not all digital communications using PKCs would potentially be compromised. While the date that quantum computers will be available is uncertain, it is important for companies, organizations, government entities, and individuals to start preparing for the impending quantum computing revolution.

What is the Significance of the Aeolus VPN and PQC Integration?

Castle Shield is taking a lead posture by packaging and productizing two of the PQC candidates and integrating them into off-the-shelf products. This demonstrates that Castle Shield has the capability to package and productize PQC algorithms. Given our encryption agnostic approach, Castle Shield will focus on the two leading candidates in each category and will update our use of the PQC's as they evolve.

Specifically, the current PQC algorithms fall under two categories: Key Encapsulation Mechanism (KEM) and Digital Signature Algorithm (DS). The current PQC Finalist candidates are:

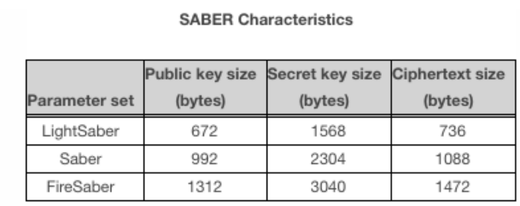
Public-Key Encryption/KEMs

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

Digital Signatures/DSAs

- CRYSTALS-DILITHIUM
- FALCON
- RAINBOW

Castle Shield implemented PQC SABER/KEM into Aeolus VPN. SABER characteristics include the following:



SABER Characteristics

Parameter set	Public key size (bytes)	Secret key size (bytes)	Ciphertext size (bytes)
LightSaber	672	1568	736
Saber	992	2304	1088
FireSaber	1312	3040	1472

Customers can choose which SABER parameter to configure into Aeolus VPN based on specific requirements of their organization. Our Aeolus VPN standard PQC configuration is SABER/KEM.

A Note About Performance

Aeolus VPN with PQC is slightly faster than its non-PQC counterparts especially at a load above 250Mbps. We will go into performance testing results in our next press release. The key takeaway is that Aeolus VPN with or without PQC performs in-line or better as compared to popular open-source VPNs.

Additional PQC Packages and Productizations are on the Horizon

Castle Shield has also packaged and productized CRYSTALS-DILITHIUM/DSA. We are in the late stages of testing, and we will announce the availability of product(s) using CRYSTALS-DILITHIUM/DSA at a later date. With SABER/KEM and CRYSTALS-DILITHIUM/DSA, we now have a PQC algorithm for both the KEM and DSA categories.

In Closing

“While many corporations and government agencies are focused on the asymmetric key exchange when preparing for the quantum era, Castle Shield has adopted a holistic cryptographic approach by including quantum-resistant encryption algorithms for both asymmetric and symmetric ciphers. It is true that symmetric ciphers, like the Advanced Encryption Standard (AES), are thought to be less vulnerable in the early part of the quantum era; however, Castle Shield has decided to offer solutions with both asymmetric (PQC) and symmetric encryption that are mathematically quantum-resistant. Customers can choose to enable both types of encryptions based on their specific needs. Castle Shield is currently the only cybersecurity solutions provider to offer quantum-resistant algorithms for both. In a world where data breaches, ransomware, and other cyberattacks are occurring daily, protecting our customer’s most valued asset, their data, should not be left to chance,” said Dr. Milton Mattox, Chief Technology Officer at Castle Shield, Holdings, LLC.

Aeolus VPN with PQC is available today for beta testing and proofs of concept. Customers may choose any one of the symmetric ciphers based on their needs. Aeolus VPN with PQC runs on Linux, Windows, macOS and works with both TCP and UDP which enables enterprises to securely encrypt point-to-point data-in-motion connections without compromising performance and flexibility. Lastly, the Castle Shield packaged PQC SABER/KEM library solution is also available to vendors and customers who wish to integrate PQC into their solutions.

22. Why Do We Care About Quantum Computers at All?

by Frank Zickert
https://towardsdatascience.com/why-do-we-care-about-quantum-computers-at-all-403dd6191c2b

Allegedly, quantum computers can do things that classical computers can't. A phenomenon we describe as quantum supremacy. Yet, even tech giants despair in the pursuit of it. Why do Google, IBM, Microsoft, and others act like donkeys with a carrot dangled before their nose?

It is all his fault! OK, not all of it. But a lot. In 1994, Peter Shor formulated his famous quantum algorithm that factors integers exponentially faster than any known classical algorithm. It caused a lot of excitement beyond academia because modern encryption builds upon the fact that it takes thousands of years to find the prime factors of an arbitrarily large number. If we could factor such numbers in a few minutes, prime-factor-based encryption collapsed like a house of cards.

Apparently, we haven't experienced this apocalypse yet. Shor's algorithm is unsuited to prove quantum supremacy in practice today. Be assured nobody can read your encrypted messages. Except for the NSA, maybe. The simple reason is that Shor's algorithm needs millions of error-corrected qubits to factor a number we're talking about. State-of-the-art quantum computers have about 100 qubits. And, these are error-prone, too.

So, our secrets remain secure for a while. Yet, the competition for proving quantum supremacy in practice has heated up. In 2019, Google reported that their 53-qubit quantum device "Sycamore" solved a task in a few minutes that would take today's most powerful supercomputers thousands of years.

IBM, a major competitor in the development of quantum computers, objected immediately. They argued their classical supercomputers could do the same task in 2.5 days. If you ask me, solving a task in minutes that a supercomputer takes days is still very impressive. Yet, it is not what we mean by quantum supremacy.

Where do such extraordinary expectations come from?

Quantum supremacy does not mean a slight advantage. On the contrary, it implies that the speed of a quantum computer vastly exceeds that of classical computers. But, why do we expect that? In other words, why should a quantum computer be faster than a classical computer?

The predominant explanation of a quantum computer's advantage over a classical computer is that we can prepare quantum bits in a superposition of an exponential number of states. Then, the quantum algorithm computes all possible inputs at the same time.

Sounds great. Yet, it appears pretty anecdotal. And, unfortunately, the description often ends at this point. If quantum computers can compute an exponential number of states concurrently, why don't we see them everywhere? I mean, with 53 qubits, we could compute 2^53=9,007,199,254,740,992 states — at once.

Ok, we can see where the expectations come from. But then, where's the problem?

Why do they all struggle with exploiting the advantages of a quantum computer?

Another popular explanation pins down the advantage of quantum computers based on the machinery of the computational complexity theory. Complexity theory is the study of the computational effort required to run an algorithm. And, what makes quantum computing so powerful is the algorithms it makes possible. Quantum algorithms may exhibit different complexity characteristics than their classical equivalents.

For instance, the computational effort of addition is O(n). This means that the effort of adding two numbers increases linearly with the size (digits) of the number. The computational effort of multiplication is $O(n^2)$. The effort increases by the square of the number size. These algorithms are said to be solvable in polynomial time. Therefore, they belong to class P problems.

But these problems are comparably simple. In contrast, the best classical algorithm for solving the problem of factorization, finding the prime factors of an n-digit number, is O(e^{n^{1/3}}). It means that the effort increases exponentially with the number of digits.

This is the difference between O(e^{n^{1/3}}) (factorization) and $O(n^2)$ (multiplication) complexity. It must not be underestimated. While your smartphone can multiply numbers with 800 digits in a few seconds, the factorization of such numbers takes about 2,000 years on a supercomputer.

The complexity illustrates vividly what we expect from a quantum computer. And the race for quantum supremacy continues.

Very recently, in 2021, a Chinese team claimed their quantum computer “Zuchongzhi” solved a problem in an hour that would have taken eight years classically. Quite astonishing.

Nevertheless, we do not experience the effects of quantum supremacy in our everyday lives. That’s because there’s a catch! The tasks “Sycamore” and “Zuchongzhi” solved were purposely designed to demonstrate the quantum computer’s superiority. These problems aren’t of much practical interest otherwise. We’re still waiting for someone to demonstrate solving a relevant problem with a quantum computer.

But why is it so hard to solve relevant problems with a quantum computer?

If you have taken the trouble to calculate the examples above, you’ll have noticed that the multiplications are the results of the factorization problems. So, interestingly, the complexity of factorization grows exponentially. But if you know the solution, you can verify that it is correct in polynomial time. Then, we say the overall problem has a non-deterministic polynomial (NP) complexity.

So, while the evaluation of a candidate is easy and straightforward, the complexity originates from selecting the correct answer out of an exponentially growing number of candidates. And, this is where the first explanation of quantum supremacy comes into play. Remember, the number of states a quantum computer can evaluate concurrently grows exponentially with the number of qubits.

In layman’s terms, we remove the “non-deterministic” from non-deterministic polynomial complexity. And, a polynomial complex task is easy to solve. But this removal is not as easy as it sounds. It is a challenging task. There are many known NP-hard problems, such as the boolean satisfiability problem, the traveling salesman problem, or the max-cut problem. Developing an algorithm that exploits the potential quantum supremacy requires a deep understanding of the problem and where its specific complexity comes from.

For instance, Peter Shor knew that the Fourier Transform operation was a good tool to find frequencies and that it is useful to solve factorization. His true achievement then was the discovery of the Quantum Fourier Transform.

But we can’t use the same technique to solve other NP-hard problems. We need savvy domain experts who understand enough of the problem and the specificity of quantum algorithms to discover how to solve them.

Apparently, this is a complex problem.

23.How to Prepare Your PKI for Quantum Computing

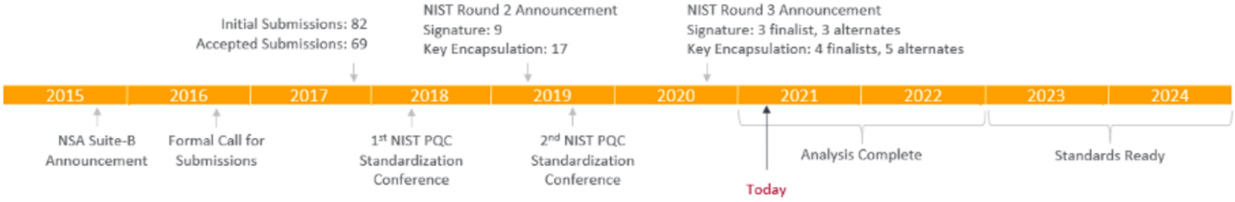
by Mike Brown
https://www.venafi.com/blog/how-prepare-your-pki-quantum-computing?utm_medium=email&_hsmi=174804691&_hsenc=p2ANqtz-_Hr4RSryefvVYjpqM7yYF-e1qo_LaC6xx_G2ljot91Djyiwqsv2OUa3nHOUOkg44XlMUM1wHC3ijvDq2NQLso4mB8tsA&utm_content=174804691&utm_source=hs_email

In my first blog in this series on quantum preparedness, I talked about the urgency of taking early steps to get ready for this radical change in the way that we think about and manage machine identities. In this blog, I'll give you some practical advice about how you can prepare your PKI for quantum computers.

One of the reasons we're worried about quantum computers is that they're really good at one specific math problem. But it's a big one and one that could eclipse everything that we know today. NIST in the United States, and others, are focused on what we should replace that math problem with, and by extension, what the new solution is going to be. In particular, NIST is leading the effort around the standardization through the FIPS program — what's known as post-quantum cryptography.

I want to reiterate that we won't be able to rely upon RSA and ECC once large-scale quantum computers arrive, so the work now is around the new math constructs that we're going to use to compensate. There are about five different math areas that we're focused on as an industry. Let's look at how we can use those fundamental math problems to construct cryptographic solutions. Specifically, we need to make sure that we spend enough time and have enough eyeballs on quantum to know what we can trust — and then standardize them so that everyone knows how to use cryptography as a language.

We rely on the language of cryptography to communicate securely. That's why standards are enormously important to make sure that we all agree upon the language we're using, and that we all know the grammar to use to talk to each other clearly. This is a complex and challenging problem! NIST started the process back in 2016. If you look at that timeline across the bottom of figure 1, you can see we're currently into what's known as "round three," where we're looking at some finalist candidates, some alternates, and NIST has recently indicated that it should have the first round of standards ready in late 2022. In parallel to this, NIST has an effort that has been looking at something called stateful hash-based signatures.


Initial Submissions: 82
Accepted Submissions: 69
NIST Round 2 Announcement
Signature: 9
Key Encapsulation: 17
NIST Round 3 Announcement
Signature: 3 finalist, 3 alternates
Key Encapsulation: 4 finalists, 5 alternates
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
NSA Suite-B Announcement
Formal Call for Submissions
1st NIST PQC Standardization Conference
2nd NIST PQC Standardization Conference
Today
Analysis Complete
Standards Ready

Stateful hash-based signatures are a very good solution for some specific use cases, such as code signing where there aren’t too many signatures. We've been working with a lot of the industry leaders from a security infrastructure perspective to make sure that these types of solutions are ready so that as organizations start to deploy them, their infrastructure is ready.

PKI is complicated, but it's not complicated in terms of drawing the org chart on a white board to illustrate what your Root CA, intermediate CA and end user certificates look like. It's complicated in terms of how it's used by systems.

If we think about an example in the U.S., the U.S. Department of Defense has over four and a half million users on its PKI, and it is using certificates to access benefits through the U.S. Department of Veterans Affairs. They use these machine identities for physical access control into bases with a common access card. They also use them for storing credentials for secure email. If we think about how we start to change and migrate the mathematics that we use from a crypto perspective, the concern is less about the actual certificate itself and more about the compatibility of that machine identity.

That's a protocol-type problem. It becomes a kind of backwards and forwards compatibility problem. Because when we have millions of users, we can't just upgrade all the systems overnight. This is going to be a multi-year, staged upgrade, and you want to simplify this process as much as possible — and make it as seamless to the end-users as possible.

The technology that we've been looking at is something we call ISARA Catalyst, which is an agile methodology that utilizes the existing X.509 certificate format with existing classic algorithms, but also includes a quantum-safe signature in the extension to allow you to have something that's backwards compatible and allows you to upgrade systems in a stepwise fashion. This enables you to be ready for quantum, so you can start trialing out quantum-safe solutions. This will allow you to start making sure that your systems are prepared for any types of changes you may need to make in order to become quantum safe.

PKI is obviously part of it, but as an organization one of the other pieces that is extremely important is thinking about how to start to look at the actual cryptography itself. With new quantum-safe solutions, we're going to have pros and cons and use cases where some math areas may solve certain problems better than other math areas. Some might be safer, but at the expense of larger key sizes, and others might be faster but may have potentially less security associated with them.

What we offer through the ISARA toolkit is the ability for customers to start testing things out now. When we talk to people that are thinking about how they get their systems ready for quantum safety, they want to start seeing what the impact of the new math systems are going to be. They want to make sure that the hardware they have is going to be good enough and that the networking protocols that they're relying upon are going to be ready when large-scale quantum computers arrive.

Machine Identities and Quantum Safety

How do you know you're ready for quantum safety? And how do you get these solutions in front of your clients? This is the work that Venafi and Crypto4A have been doing together via VCert and the Venafi Platform. We've been working together to make sure that you can utilize VCert to start generating keys using NIST candidate algorithms. You can start creating CSRs and certificates that use hybrid technologies. At that point, you can start seeing how quantum safe certificates might work within your environment and understand what things need to be upgraded and what things are going to work great with quantum. This is the sort of normal IT migration problem that you need to think through!

An essential part of this solution is thinking about how to start to issue certificates that are quantum-ready. This is the Crypto4A quantum safe certificate service. We've been working very closely with Crypto4A about how a hardware appliance will help you issue certificates in a quantum-safe environment.

We already have protections that use the Venafi Platform with Crypto4A and ISARA. You can start to prepare your infrastructure to make sure that it is ready to be quantum safe and we'll also allow you to start testing things out. But it's also important to prepare for an agile transition. As an industry, we've gone through crypto transitions a number of times before — Triple DES to AES, MD5 hash functions and SHA-1 to SHA-2. But this one will be bigger. Changes in key sizes as well as this quantum-safe transition is the largest transition we've had to think about from a cryptographic perspective. It certainly won't be the last transition, so this is our opportunity to make sure that while we're testing, and while we're getting your infrastructure ready for quantum, we can also start planning for what's the next transition and how do we make sure that we're ready for it.

24.Quantum networking milestone in real-world environment

by DOE/Oak Ridge National Laboratory
https://www.sciencedaily.com/releases/2021/10/211007122111.htm

A team from the U.S. Department of Energy's Oak Ridge National Laboratory, Stanford University and Purdue University developed and demonstrated a novel, fully functional quantum local area network, or QLAN, to enable real-time adjustments to information shared with geographically isolated systems at ORNL using entangled photons passing through optical fiber.

This network exemplifies how experts might routinely connect quantum computers and sensors at a practical scale, thereby realizing the full potential of these next-generation technologies on the path toward the highly anticipated quantum internet. The team's results, which are published in *PRX Quantum*, mark the culmination of years of related research.

Local area networks that connect classical computing devices are nothing new, and QLANs have been successfully tested in tabletop studies. Quantum key distribution has been the most common example of quantum communications in the field thus far, but this procedure is limited because it only establishes security, not entanglement, between sites.

"We're trying to lay a foundation upon which we can build a quantum internet by understanding critical functions, such as entanglement distribution bandwidth," said Nicholas Peters, the Quantum Information Science section head at ORNL. "Our goal is to develop the fundamental tools and building blocks we need to demonstrate quantum networking applications so that they can be deployed in real networks to realize quantum advantages."

When two photons -- particles of light -- are paired together, or entangled, they exhibit quantum correlations that are stronger than those possible with any classical method, regardless of the physical distance between them. These interactions enable counterintuitive quantum communications protocols that can only be achieved using quantum resources.

One such protocol, remote state preparation, harnesses entanglement and classical communications to encode information by measuring one half of an entangled photon pair and effectively converting the other half to the preferred quantum state. Peters led the first general experimental realization of remote state preparation in 2005 while earning his doctorate in physics. The team applied this technique across all the paired links in the QLAN -- a feat not previously accomplished on a network -- and demonstrated the scalability of entanglement-based quantum communications.

This approach allowed the team to link together three remote nodes, known as "Alice," "Bob" and "Charlie" -- names commonly used for fictional characters who can communicate through quantum transmissions -- located in three different research laboratories in three separate buildings on ORNL's campus. From the laboratory containing Alice and the photon source, the photons distributed entanglement to Bob and Charlie through ORNL's existing fiber-optic infrastructure.

Quantum networks are incompatible with amplifiers and other classical signal boosting resources, which interfere with the quantum correlations shared by entangled photons. With this potential drawback in mind, the team incorporated flexible grid bandwidth provisioning, which uses wavelength-selective switches to allocate and reallocate quantum resources to network users without disconnecting the QLAN. This technique provides a type of built-in fault tolerance through which network operators can respond to an unanticipated event, such as a broken fiber, by rerouting traffic to other areas without disrupting the network's speed or compromising security protocols.

"Because the demand in a network might change over time or with different configurations, you don't want to have a system with fixed wavelength channels that always assigns particular users the same portions," said Joseph Lukens, a Wigner Fellow and research scientist at ORNL as well as the team's electrical engineering expert. "Instead, you want the flexibility to provide more or less bandwidth to users on the network according to their needs.”

Compared with their typical classical counterparts, quantum networks need the timing of each node's activity to be much more closely synchronized. To meet this requirement, the researchers relied on GPS, the same versatile and cost-effective technology that uses satellite data to provide everyday navigation services. Using a GPS antenna located in Bob's laboratory, the team shared the signal with each node to ensure that the GPS-based clocks were synchronized within a few nanoseconds and that they would not drift apart during the experiment.

Having obtained precise timestamps for the arrival of entangled photons captured by photon detectors, the team sent these measurements from the QLAN to a classical network, where they compiled high-quality data from all three laboratories.

"This part of the project became a challenging classical networking experiment with very tight tolerances," Lukens said. "Timing on a classical network rarely requires that level of precision or that much attention to detail regarding the coding and synchronization between the different laboratories.”

Without the GPS signal, the QLAN demonstration would have generated lower quality data and lowered fidelity, a mathematical metric tied to quantum network performance that measures the distance between quantum states.

The team anticipates that small upgrades to the QLAN, including adding more nodes and nesting wavelength-selective switches together, would form quantum versions of interconnected networks -- the literal definition of the internet.

"The internet is a large network made up of many smaller networks," said Muneer Alshowkan, a postdoctoral research associate at ORNL who brought valuable computer science expertise to the project. "The next big step toward the development of a quantum internet is to connect the QLAN to other quantum networks.”

Additionally, the team's findings could be applied to improve other detection techniques, such as those used to seek evidence of elusive dark matter, the invisible substance thought to be the universe's predominant source of matter.

"Imagine building networks of quantum sensors with the ability to see fundamental high-energy physics effects," Peters said. "By developing this technology, we aim to lower the sensitivity needed to measure those phenomena to assist in the ongoing search for dark matter and other efforts to better understand the universe.”

The researchers are already planning their next experiment, which will focus on implementing even more advanced timing synchronization methods to reduce the number of accidentals -- the sources of noise in the network -- and further improve the QLAN's quality of service.

25.IonQ has a Working Quantum Computer that Operates at Room Temperature

by Steven Leibson
https://www.eejournal.com/article/ionq-has-a-working-quantum-computer-that-operates-at-room-temperature/

I know I’ll be in trouble for saying this, but Professor Christopher Monroe gave a presentation about IonQ’s Quantum computing element at Hot Chips 33, and I very nearly understood it. That does not usually happen when I listen to quantum explanations, which usually end up as a superposition of many understood, poorly understood, and completely misunderstood ideas. I don’t think it’s my fault. Understanding the fundamentals of quantum computing is hard. Implementing a working quantum computer is even harder.

Not Normal

Quantum computers don’t use bits like normal digital computers; they use quantum bits or “qubits.” Not a “cubit.” That’s the measurement system that Noah used to design and build his ark. That system is based on the distance between the elbow and the tip of the middle finger, and it’s supposedly 18 inches or 44 cm, although the particular arm you use to make measurements probably changes the measure significantly. Qubits can simultaneously store zeroes and ones in various proportions. This capability is known as superposition: the values are overlaid in the qubit. Because of this superposition, 300 qubits can store more combinations than there are particles in the universe, so qubits can help us work with large numbers, if we can tame them.

The most obvious use for qubit-based quantum computing is for factoring large numbers. Digital computers are not very good for this application, which is a good thing because modern cryptography depends on the current difficulty in factoring large numbers. The math tells us that quantum computers should be exponentially faster than digital computers when factoring large numbers.

However, quantum computers will be useful for applications well beyond cryptography, including protein folding (for drug research and discovery) and for solving combinational optimization questions such as the traveling salesperson problem, which asks, “What is the shortest path a salesperson can take to visit N cities?” When the number N is small, optimization is fairly easy. When N grows larger, the number of combinations explodes and quickly grows beyond solution by conventional computing.

I’m not about to display my quantum ignorance in this short article. Instead, I’m about to discuss some really interesting developments at Professor Monroe’s company, IonQ. They’re developing a quantum computer. In and of itself, that’s not really big news. Lots of organizations including many universities, Intel, IBM, and Microsoft are developing quantum computers that involve several tons of hardware including cryogenic refrigeration. That’s because most approaches to quantum computing need to chill the circuitry down to near absolute zero to maintain qubit coherency.

Oh darn. Now I have to explain quantum coherency.

Here’s the short version: Qubits can interact with each other. Without interaction, a quantum system can remain in steady state – it maintains coherence. When qubits affect each other, the system they reside in can change state, which results in decoherence. Once the state is lost, you have to start over. Cryogenic temperatures increase the amount of time that most quantum systems can remain coherent.

The only way to do all of this is to use identical parts for each qubit. Wires cannot be made identical; transistors cannot be made identical; Josephson junctions cannot be made identical. So IonQ uses individual ionized rare-earth ytterbium atoms floating inside of an ion trap within a vacuum as qubits. Atoms of the same element (and the same isotope) are identical, so they make great qubits, according to Monroe. According to IonQ’s Website, ytterbium atoms are “so consistent they’re used in one of the most accurate atomic clocks ever built.”

It’s all done with lasers

So how does IonQ deal with coherence? They appear to have sidestepped the problem entirely by basing their qubits on individual atoms. Using atoms (or ions actually), IonQ has developed a system that chills the individual ions to near-absolute-zero levels using Doppler cooling and other laser-based cooling techniques while the apparatus operates at room temperature. The ions cool as they absorb and emit photos. No giant refrigeration unit needed.

The qubit atoms enter an ion trap where they’re manipulated in groups and individually by lasers. A laser strips each ytterbium atom of one electron to create an ion so that the atom can be held in place electromagnetically by a linear ion trap.

“It’s impossible to create a trapping force with electrodes at fixed voltages that can hold an ion in a fixed position. Instead, we use rapidly oscillating voltages, such that the average field traps the ions in all three dimensions. As an analogy, imagine placing a ball on top of a saddle, and then spinning the saddle very quickly — it’s the same basic idea.”

The current ion trap design uses about 100 electrodes to hold the ions in place. The electrodes are formed by depositing gold on silicon and etching patterns using conventional lithographic techniques.

IonQ then uses lasers to put the trapped ytterbium ions in a particular quantum state of superposition, which is stored in each atom’s spin. Once placed in a particular stable quantum state, the atoms can remain in that state for very long periods of time, even at room temperature, as long as they’re held in the ion trap. IonQ also uses lasers to perform operations on the qubits and to read out a final answer. Monroe described these operations as “gates.” For IonQ’s purposes, a gate is one operation on one or more ions. IonQ’s quantum computer performs operations on these ions using an array of individual laser beams, each imaged onto an individual ion, plus one global laser beam that strikes all of the ions in the trap simultaneously. The interference between the individual and global laser beams produces a beat note that provides exactly the necessary energy to kick the qubit ions into a different state.

Once the computations are completed, a resonant global laser illuminates all of the ions at the same time, which collapses any complex quantum information created by the computations and forces each qubit into one of two states.

The collapsed state is the calculation result. The ions will glow or not glow when energized, depending on whether they're in the "one" state or the "zero" state. Collecting and measuring this emitted light allows IonQ to simultaneously read the collapsed state of every ion, and the string of glowing ions is interpreted as the computational result: a binary string, where each glowing atom is a one, and each dark atom is a zero.

Passing a computation through several gates takes place over time, as opposed to a digital circuit design where data flows spatially across a circuit board through a series of gates. According to IonQ's Website, the company has run single-qubit gates on a 79-ion chain and has complex algorithms on chains of as many as 11 ions. The company is currently working on a system that will operate 32 qubits simultaneously, and the end goal is to produce operational systems compatible with existing data centers by the year 2025. Monroe also commented that IonQ is set to become a public company this year.

26.Quantum Company Rigetti Computing to Go Public via SPAC

https://insidehpc.com/2021/10/quantum-company-rigetti-computing-to-go-public-via-spac/

Rigetti & Co., Inc. ("Rigetti"), a pioneer in full-stack quantum computing, announced today it has entered into a definitive merger agreement with Supernova Partners Acquisition Company II, Ltd. ("Supernova II"), a publicly traded special purpose acquisition company. When the transaction closes, the publicly traded company will be named Rigetti Computing, Inc. and its common stock is expected to be listed on the NYSE under the ticker "RGTI."

Rigetti is a leader in scalable quantum processor technology. Scalability has been among the largest hurdles to bringing quantum computing to market, and Rigetti introduced its scalable superconducting chips in June 2021. Its patented multi-chip architecture is the building block for new generations of quantum processors that are expected to achieve a clear advantage over classical computers.

Quantum computing is one of the most transformative emerging technologies in the world today. Many of the world's most important problems remain intractable, lying far beyond the capabilities of today's supercomputers. Quantum computers process information in a fundamentally different way — solving problems simultaneously as opposed to sequentially — which will allow them, when scaled, to tackle problems of staggering computational complexity at unprecedented speed.Quantum computing could be applied to a range of important uses such as enabling biotech companies to bring more effective therapies to market faster; researchers to develop more affordable clean energy sources; and financial companies to access faster and more accurate market insights to help reduce market volatility.

Rigetti will use the proceeds from the transaction to accelerate development of multiple generations of quantum processors and grow its commercial business. Rigetti expects to scale its quantum computers from 80 qubits in 2021, to 1,000 qubits in 2024, and to 4,000 qubits in 2026.Rigetti's distinctive quantum computers work in tandem with existing cloud and high-performance computing infrastructure to unlock powerful new capabilities to solve complex real-world problems. The company sells access to its machines through the Rigetti Quantum Cloud Services platform.

The PIPE transaction is subscribed to by top investors including: funds and accounts advised by T. Rowe Price Associates, Inc.; Bessemer Venture Partners; Franklin Templeton; and In-Q-Tel. Strategic investors include Keysight Technologies and Palantir Technologies. Ampere Computing will make a direct investment. These new strategic investors provide strong complementary technologies for advancing Rigetti's quantum advantage, and build on Rigetti's existing partnerships and collaborations with customers like Amazon Web Services, Astex Pharmaceuticals, DARPA, NASA, Standard Chartered Bank and the U.S. Department of Energy.

Rigetti CEO Chad Rigetti founded the company in 2013. The company has raised approximately $200 million in venture capital and today employs more than 130 people with offices in the United States, Canada, U.K., and Australia.Supernova II is led by Michael Clifton, an investor who most recently helped lead global technology investing at The Carlyle Group; Robert Reid, a long-time senior partner at Blackstone; Spencer Rascoff, a serial entrepreneur who co-founded Hotwire, Zillow, dot.LA and Pacaso and who led Zillow as CEO for nearly a decade; and Alexander Klabin, founder and CEO of Ancient and former managing partner, co-CIO and co-founder of Senator Investment Group.Clifton is expected to join the Rigetti Board of Directors after the transaction closes.

"In the next decade one Rigetti quantum computer could be more powerful than today's entire global cloud. Rigetti is the leading innovator in this space. Our team has solved the most pressing scientific problems associated with bringing quantum computing to market by creating a scalable computer and high-performance integration with existing computing systems. We plan to use this capital to accelerate our product development and accelerate our goal to bring this transformational computing capability to every major industry."Michael Clifton, Supernova II

"The widespread adoption of quantum computing will have a significant impact on the economy and humanity in the next decade and beyond, on par with the advent of mobile and cloud technologies. Rigetti systems 'speed and scalability set them apart amongst competitors. With its model of easy integration into existing systems, Rigetti's technology will be used by businesses, governments and institutions across the globe."

27.JPMorgan's guide to quantum machine learning in finance

by Sarah Butcher
https://www.efinancialcareers.com/news/2021/10/quantum-machine-learning-banking

We suggested in January that it might be a good idea to familiarize yourself with quantum computing if you want to maximize your future employability in financial services. A new academic paper from JPMorgan's Future Lab for Applied Research and Engineering helps explain why.

Authored by Marco Pistoia, JPMorgan's head of quantum technology and head of research, plus members of his team, the paper stresses that quantum computing will impact financial services sooner than you think. Goldman Sachs and JPMorgan have both been building teams of quantum researchers and Goldman has already used quantum methods to speed up derivatives pricing by over a thousand times. The finance industry stands to benefit from quantum computing "even in the short term," says JPMorgan.

The researchers note banks and finance firms are already big users of machine learning techniques like reinforcement learning for algorithmic trading, or Natural Language Processing (NLP) for risk assessment, financial forecasting and accounting and auditing. Many of the machine learning techniques using quantum methodologies, but talent remains hard to find. "Demand is high and quantum is still a very rare skill," says one senior banking technologist.

(i) **Asset pricing:** Banks have been using Recurrent Neural Networks (RNNs) to run time series predictions and are considering using them for asset pricing models, says JPMorgan. However, RNNs consume a lot of computing power, and there are advantages to using parameterized quantum circuits (PQCs) and quantum Long Short Term Memory (LSTM) units that allow users to make predictions about evolving processes from historical data.

(ii) **Predicting volatility:** Quantum methods can also be used to determine the likely changes in a security's price. Deep quantum neural networks produce a density matrix, and the implied volatility of an option is calculated using its respective element in the matrix.

(iii) **Predicting the outcome of exotic options:** Machine learning support Vector Machines (SVMs) can be used to predict the circumstances in which exotic options used in markets like FX pay out. Quantum techniques can facilitate this.

(iv) **Fraud detection:** Quantum clustering algorithms can be used to perform anomaly detection and identify fraudulent activity.

(v) **Stock selection:** Quantum clustering algorithms can also be used to cluster stocks with similar returns but different risks, thereby allowing investors to pick low-risk stocks with high returns.

(vi) **Hedge fund selection:** The same clustering algorithms can be used to identify hedge funds for funds to invest in based on known variables like asset classes, size, fees, leverage and liquidity.

(vii) **Algorithmic trading:** Quantum reinforcement learning techniques could be applied to algorithmic trading in order to speed up decision-making and improve the complexity of models. However, the researches note that this hasn't happened yet due to the hardware limitations of current quantum devices.

(viii) **Market making:** Electronic market makers like Citadel Securities and Jane Street are likely to take an interest in quantum computing for their own reasons. "Market making is amenable to quantum reinforcement learning," says JPMorgan. - The problem is modelled as an "agent state, taking into account attributes such as inventory and risk-tolerance, and an environment state where the agent only has partial information."

(ix) **Financial forecasting, accounting and auditing and risk assessment:** JPMorgan's team predict that quantum natural language processing (NLP) algorithms are also coming for jobs in risk and accounting teams. NLP can be used, for example, to elicit "lender's and borrower's emotions during a loan process, to conduct sentiment analysis for forecasting, or to create semantic knowledge bases for financial accounting standards.

28. D-Wave plans to build a gate-model quantum computer

by Fredric Lardinois
https://techcrunch.com/2021/10/05/d-wave-plans-to-build-a-gate-model-quantum-computer/

For more than 20 years, D-Wave has been synonymous with quantum annealing. Its early bet on this technology allowed it to become the world's first company to sell quantum computers, but that also somewhat limited the real-world problems its hardware could solve, given that quantum annealing works especially well for optimization problems like protein folding or route planning. But as the company announced at its Qubits conference today, a superconducting gate-model quantum computer — of the kind IBM and others currently offer — is now also on its roadmap.

D-Wave believes the combination of annealing, gate-model quantum computing and classic machines is what its businesses 'users will need to get the most value from this technology. "Like we did when we initially chose to pursue annealing, we're looking ahead," the company notes in today's announcement. "We're anticipating what our customers need to drive practical business value, and we know error-corrected gate-model quantum systems with practical application value will be required for another important part of the quantum application market: simulating quantum systems. This is an application that's particularly useful in fields like materials science and pharmaceutical research."

Early on, the company argues, annealing provided the fastest path to building quantum applications. Today, about 250 D-Wave customers have built applications for its hardware, which virtually all of its users access through its Leap cloud service. And since there's clearly value in quantum annealing, too, D-Wave won't do away with it. "Annealing remains core to our roadmap," the company says, and it plans to continue to invest and develop its current systems. Indeed, D-Wave believes that annealing — and the optimization use cases it enables — will account for about a third of the quantum application market.

But the company is also clearly aware that this is a major change in its strategy and that it has a bit of explaining to do. For years, after all, D-Wave argued that its annealing technology might one day be able to be used for a general quantum computer, too. Now, however, the company notes that since the technology and theory behind it has matured — and D-Wave itself has learned a lot about the materials engineering challenges involved — it's "exactly the right time from a technical and theory perspective to face the challenges of gate-model implementation head-on."

D-Wave is also quite open about the fact that this isn't going to be a straightforward journey. After all, this is still quantum computing we are talking about. Given this, it's not surprising that the company's roadmap for its gate-model processor doesn't feature any dates, but instead phases that range from building a first qubit (phase 1) to building a general-purpose quantum processing unit (QPU).

While the gate-model news is obviously the headline event today, D-Wave also made a few other announcements. It's launching a performance update to its latest 5,000+ qubit Advantage-class machines today, for example, that promises to allow its users to solve larger and more complex problems. It's also launching its Constrained Quadratic Model (CQM) solver today, which complements the existing range of solvers in D-Wave's Leap service.

As for its overall roadmap, D-Wave expects to launch its latest Advantage machine with over 7,000 qubits — which will have a new design, too — and 20-way connectivity in a new topology, somewhere around 2023 or 2024, for example. And starting next year, it plans to launch new hybrid solvers that can solve mixed integer problems to help its users tackle more drug trial and chemical process optimization, logistics, scheduling and similar problems.

The real end-goal here, though, is to be able to offer a deeply integrated stack that offers its customers access to a set of hardware and software options that will allow them to tackle virtually any problem in quantum computing.

“Our full-stack approach to quantum technology, everything from chip fabrication to system development, and from hybrid software solvers to robust open source developer tools, means that we’re the only company in the world that can both deliver on regular product innovations and bring a cross-platform stack to market quickly. That’s practical,” said D-Wave CEO Alan Baratz.

29. Scientists are one step closer to error-correcting quantum computers

by Emily Conover
https://www.sciencenews.org/article/quantum-computer-error-correction-multiple-qubits-detect-mistakes

Mistakes happen — especially in quantum computers. The fragile quantum bits, or qubits, that make up the machines are notoriously error-prone, but now scientists have shown that they can fix the flubs.

Computers that harness the rules of quantum mechanics show promise for making calculations far out of reach for standard computers. But without a mechanism for fixing the computers ’mistakes, the answers that a quantum computer spits out could be gobbledygook.

Combining the power of multiple qubits into one can solve the error woes, researchers report October 4 in *Nature*. Scientists used nine qubits to make a single, improved qubit called a logical qubit, which, unlike the individual qubits from which it was made, can be probed to check for mistakes.

“This is a key demonstration on the path to build a large-scale quantum computer,” says quantum physicist Winfried Hensinger of the University of Sussex in Brighton, England, who was not involved in the new study.

Still, that path remains a long one, Hensinger says. To do complex calculations, scientists will have to dramatically scale up the number of qubits in the machines. But now that scientists have shown that they can keep errors under control, he says, “there’s nothing fundamentally stopping us to build a useful quantum computer.”

In a logical qubit, information is stored redundantly. That allows researchers to check and fix mistakes in the data. “If a piece of it goes missing, you can reconstruct it from the other pieces, like Voldemort,” says quantum physicist David Schuster of the University of Chicago, who was not involved with the new research. (The *Harry Potter* villain kept his soul safe by concealing it in multiple objects called Horcruxes.)

In the new study, four additional, auxiliary qubits interfaced with the logical qubit, in order to identify errors in its data. Future quantum computers could make calculations using logical qubits in place of the original, faulty qubits, repeatedly checking and fixing any errors that crop up.

To make their logical qubit, the researchers used a technique called a Bacon-Shor code, applying it to qubits made of ytterbium ions hovering above an ion-trapping chip inside a vacuum, which are manipulated with lasers. The researchers also designed sequences of operations so that errors don't multiply uncontrollably, what's known as "fault tolerance."

Thanks to those efforts, the new logical qubit had a lower error rate than that of the most flawed components that made it up, says quantum physicist Christopher Monroe of the University of Maryland in College Park and Duke University.

However, the team didn't quite complete the full process envisioned for error correction. While the computer detected the errors that arose, the researchers didn't correct the mistakes and continue on with computation. Instead, they fixed errors after the computer was finished. In a full-fledged example, scientists would detect and correct errors multiple times on the fly.

Demonstrating quantum error correction is a necessity for building useful quantum computers. "It's like achieving criticality with [nuclear] fission," Schuster says. Once that nuclear science barrier was passed in 1942, it led to technologies like nuclear power and atomic bombs.

As quantum computers gradually draw closer to practical usefulness, companies are investing in the devices. Technology companies such as IBM, Google and Intel host major quantum computing endeavors. On October 1, a quantum computing company cofounded by Monroe, called IonQ, went public; Monroe spoke to *Science News* while on a road trip to ring the opening bell at the New York Stock Exchange.

The new result suggests that full-fledged quantum error correction is almost here, says coauthor Kenneth Brown, a quantum engineer also at Duke University. "It really shows that we can get all the pieces together and do all the steps."

30. QNu Labs Launches Quantum-Safe Cryptographic Keys to Secure Critical Data of Enterprises

https://www.power-technology.com/research-reports/qnu-labs-launches-quantum-safe-cryptographic-keys-to-secure-critical-data-of-enterprises/

Concept: India's technology startup QNu Labs has launched a security platform powered by quantum technology to encrypt IP data using random cryptographic numbers. The startup offers the quantum random number generator (QRNG) called Tropos and the quantum key distribution system (QKD) called Armos to address the issues around data security and privacy of vulnerable systems and networks.

Nature of Disruption: The platform leverages quantum physics to provide a new model to protect data and network. Tropos uses quantum mechanics to generate truly random numbers, which can help in various applications like one-time pad, lotteries and key generation in cryptography. Armos provides unconditional protection to data while securing the distribution of symmetric one-time pad encryption keys. It uses quantum encoding single photons of light that are sent through a dedicated fiber optical channel. It separates the encryption key from the data and directs it on a dedicated quantum channel. The symmetric key encryption monitors real-time threats on quantum keys and provides intrusion detection to block any kind of possible hacking activities. Any product changes identified in the quantum state of the keys will prompt Armos to initiate an alert and issue an accurate on-time report on the intrusion location. Armos instantly destroys compromised keys and generates a pair of quantum-safe cryptographic keys between two remote parties through an exchange of unhackable encoded quantum bits (qubits). As the keys cannot be cloned, the data remains unconditionally secured even if it is exposed.

Outlook: The current method of public-key encryption remains highly vulnerable, as hackers can easily execute ‘Harvest Now, Decrypt Later ’attack, in which they can copy, store and decrypt encrypted data at a later point of time. QNu Labs ’innovative quantum technology-powered solution can address the increasing issues around data security and privacy by deploying unhackable cryptographic keys, capable to secure critical data of enterprises, governments, finance and defense across the globe. The system employs a REST-ful API driven infrastructure that enables it to integrate with existing security suites. The startup has plans to increase its reach across WAN through satellite-based QKD and build solutions such as three-factor authentication using QRNG and QKD for digital transactions or secure blockchain Miniaturise QKD to go into a server or on to a device for 5G networks.

31. Quantum resistant protocols for Zero-Knowledge proofs to strengthen Blockchain Security

by CRN Team
https://www.crn.in/news/quantum-resistant-protocols-for-zero-knowledge-proofs-to-strengthen-blockchain-security/

Researchers at Technology Innovation Institute (TII) in the United Arab Emirates have improved the feasibility of a new class of algorithms to protect blockchain applications against quantum computing cryptographic attacks. This builds on the considerable research already underway across the cryptographic community in developing better protocols for improving zero-knowledge proofs.

The specialised area of cryptography has been gaining significant interest since zero-knowledge proofs are widely used in techniques like blockchain, smart contracts, and identity verification.

The most popular approaches have involved using matrix computations. However, there is some concern that future research may find new and improved ways to compromise these protocols. So, researchers are always looking for promising alternatives to provide multiple types of protection against future cryptographic attacks.

Need for alternative approaches

The various types of quantum-resistant problems and algorithms built on them are considered safe at the present time, because no one has demonstrated a credible quantum computer attack against them. Emanuele Bellini, Lead Cryptographer at TII, said: “We are in the early stages of understanding what is quantum-resistant and what is not. The safest approach is to build the quantum-resistant scheme based on many different problems so that if one is broken, you are still hopeful that the others are not.”

Most of the work on quantum-resistant protocols for zero-knowledge proofs has been based on lattices. Lattices are very flexible and are one of the most malleable cryptographic mathematical structures that can be applied across the board. The TII team has focused on alternatives to lattices based on the Rank Syndrome Decoding problems, which, although promising, still need more research to make them a credible solution.

Cryptography is a bit of a cat-and-mouse game, where researchers are constantly finding enhanced solutions to break protocols and more effective ways to implement them. It is not even necessary to completely break an approach to reduce its attractiveness. Bellini said, “If someone discovers an attack to the lattice problem that just slightly improves the previous attack, it means that the lattice parameters would have to become larger, and then other approaches would become relatively more efficient.”

The importance of zero-knowledge proofs

“Zero-knowledge” has recently become the most popular keyword in cryptographic papers presented at conferences. The popularity of these protocols grew in response to the enthusiasm around blockchain since this is the most common use case. In these applications, the goal is to be able to prove a statement is true without the rest of the blockchain understanding information about the exchange. The simplest implementations of zero-knowledge protocols are often used for identity verification.

A zero-knowledge-proof protocol organised the interaction between two parties in which one is the prover and the other the verifier. The two parties exchange information, and after the exchange, the prover can confirm the truthfulness of the statement, such as whether someone has enough money in a blockchain wallet for a transaction without knowing the total in the wallet. This is also done in a way that hides information from third-party observers.

Initially, the zero-knowledge-proof community focused on using classical cryptographic algorithms based on discrete logs or factorisation problems. The community has recently started exploring quantum-resistant zero-knowledge proofs.

Classical algorithms were inefficient, and the quantum-resistant implementations are even less so because they require larger keys. They also require larger parameters such as the size of the proof, the number of bits that need to be communicated between prover and verifier, and the amount of work each party must perform to build the proof. These quantum-resistant protocols might take minutes or hours to run compared to a few seconds for the protocols built on classical algorithms.

TII’s researchers studied the Rank Syndrome Decoding problem, an evolution of another technique called the Syndrome Decoding problem. Other popular quantum techniques have included the shortest vector problem, the NTRU problem, the isogenies problem, and the multivariate quadratic problem.

These different classes of problems organise numbers into a particular structure that is best suited for verifying a zero-knowledge proof built on top of the problem. The shortest vector and NTRU are similar and use lattices to encode the numbers to compute the problem’s answer. Multivariate problems use a system of polynomials to organise the calculation. The Syndrome Decoding Problem uses a linear code. The Rank Syndrome Decoding problem is similar to the Syndrome Decoding problem but organises the linear codes more efficiently.

Emanuele Bellini, Lead Cryptographer at the TII, said: “The Rank Syndrome Decoding problem is not something we invented. However, it is a newer problem than Syndrome Decoding and the lattice problems, so it is less studied.”

More efficient and adaptable

TII's researchers improved the efficiency of RSD and implemented it in a way that is more adaptable to different use cases. Their implementation is 60% smaller, and the parameters are 1% of the size compared to the state-of-the-art Syndrome Decoding implementation for a given proof. It is also considerably faster, solving one benchmark proof in 47 ms compared to 5,000 ms for Syndrome Decoding.

A key building block of this new construction is a commitment scheme that essentially requires one party to commit to a statement, such as having executed a certain amount of work, which can be verified later as part of a transaction.

TII researchers also demonstrated how this commitment scheme could be built into any kind of circuit, which is a fundamental building block for cryptographic transactions. Prior research had examined how RSD could be applied to signature schemes based on identification protocols using zero-knowledge proofs. However, the TII research is the first demonstration of how RSD could apply to any arbitrary circuit that could be used across many different applications.

An arbitrary circuit in cryptography is analogous to an electrical circuit in a computer chip in which bits are logically combined using gates that perform logical operations such as executing AND, OR, and NOT statements. Bellini said: "if you have enough of these gates, you can build any function."

The proof size required for verifying the statement grows at a quasi-linear rate. This means that larger statements require more computation to prove but not nearly as much as would be needed if the proof size grew at a quadratic or exponential rate.

A zero-knowledge proof is not the same as a mathematical proof. A mathematical proof is a deterministic process that allows someone to assert whether a statement is true or false based on certain assumptions. In contrast, a zero-knowledge proof is a probabilistic proof in which a statement is proved with a certain degree of probability. The probability of making a mistake is called the soundness error or cheating probability since it represents the risk that someone might be cheating but not caught.

This error can be made as small as possible by repeating the calculation multiple times. The current implementation's cheating probability is 2/3 on the first pass, which is insufficient to convince a verifier. However, by repeating the proof 219 times, the cheating probability drops to 1/2128, which is extremely low. "The fact that it is wrong is less probable than a meteor will fall on your head this afternoon," said Bellini.

Future research is looking at how to reduce the soundness error of the fundamental building blocks even further. But this needs to be approached cautiously since it may reduce the probability by creating a much longer proof that takes more time to execute. Bellini expects this to be doable since there are already examples of reducing the likelihood from 2/3 to 1/2 when using RSD for identification protocols. This would mean the researchers would only need to repeat the process 128-times rather than 219-times!

32. How Graphene Could Hold the Key to Household Quantum Computers

by Marzia Khan
https://www.azonano.com/article.aspx?ArticleID=5825

The carbon allotrope, graphene, has become a revolutionary material that has been used for many innovative applications, such as in electronics. Researchers from the Indian Institute of Technology and Germany have investigated developments in pristine graphene to encode and process quantum information more effectively, which could help aid the future of quantum computing. This article will provide more information on the innovative research undertaken by the researchers and investigate how graphene can be used to revolutionize the role of quantum computers.

Quantum computers can perform calculations based on the probability of an object's state before measurement and so can process more data. These types of computers can be seen in use by data analysis companies such as Google or Microsoft. However, they are seen as being high maintenance due to being large, expensive, and require very low temperatures such as -200 degrees Celsius for operation.

These limitations make quantum computers perfect for advancements, such as using pristine graphene for processing and storing quantum information. A novel development in this field could be revolutionary, with innovative improvements including smaller and simpler quantum computers that can function effectively at room temperature.

Quantum computers have gained more popularity in recent years due to the potential advantage over classical computers because of their higher performance and speed. Despite this, practical applications have limited their development leading to much theoretical investigation.

Research into Quantum Computers

Researchers from the Indian Institute of Technology (IIT), Bombay, and Max-Born Institut, Germany, have collaborated on advancing quantum computers and working on the challenges to make these computers more accessible. The research was published in the journal *Optica* March 18th, 2021.

The scientists achieved a breakthrough in valleytronics, an experimental area in semiconductors focused on the degree of freedom within 'valleys 'in the electronic band structure. Their investigations uncovered a method for performing valley operations within a single atom layer, or pristine graphene, where the carbon atoms are structured within a hexagonal sheet.

Associate Professor Gopal Dixit from IIT commented on the novel strategy to break graphene's valley symmetry through the use of light.

> "By tailoring the polarization of two beams of light according to graphene's triangular lattice, we found it possible to break the symmetry between two neighboring carbon atoms and exploit the electronic band structure in the regions close to the valleys, inducing valley polarization."
> Gopal Dixit, Associate Professor, Department of Physics, Indian Institute of Technology

This discovery shed new light on the electron valleys within graphene, which was previously not seen as viable for valley operations due to graphene's inherent symmetry. With this new research, the pioneering properties of graphene have reached new limits.

Graphene and Quantum Computers

The significance of exploiting the valleys within graphene lies within the possibility of increasing and optimizing encoding processes and processing information in a quantum computer. Flashes of light can cause electrons within the valleys to move several hundred trillion times a second, illustrating the potential of valleytronics working at petahertz rates. Such a development would be revolutionary for modern classical computers as this speed would be a million times faster.

Further research into this concept and advancing quantum computers could support the development of the electronics industry, providing effective and efficient technology which would meet the highest demand of industry leaders and consumers. Dr. Dixit added that the research undertaken by the group of scientists "*could open the door to miniature, general-purpose quantum computers that can be used by regular people, much like laptops*."

The Future of Quantum Computers

The potential of creating laptops with the technological advancement of quantum computers would greatly progress the electronics and semiconductor industry, from assisting consumers and supporting advanced needs to utilizing quantum computer technology in a more accessible manner within laboratories and research facilities. The applications of this potential innovation could significantly impact all industries, supporting all types of research without money bias.

With the challenges of this industry remaining endless, having a novel technology such as quantum computer technology within households would be revolutionary, dramatically modifying the quality of electronics introduced into the market. Providing cost-effective and quality technology to consumers to meet demands would further aid a developing, technological society.

Increasing the efficiency, speed, and reliability of technology through the possible introduction of quantum computers through graphene would be a step into a novel era of innovation.

33. Physicists Create New Technique to Control Qubits – The Building Blocks of Quantum Computing

by TIM CHRISTIE
https://scitechdaily.com/physicists-create-new-technique-to-control-qubits-the-building-blocks-of-quantum-computing/

QPhysicists David Allcock and David Wineland are founders of the new Oregon Ions Laboratory, which was recently set up in the basement of Willamette Hall. They are among 12 authors of a new paper, which is based on an experiment at the National Institute for Standards and Technology in Boulder, Colorado. Both scientists previously worked at the Colorado lab and continued to collaborate on the project after coming to the UO in 2018.

The techniques, described in the journal *Nature*, involve the use of trapped-ion quantum bits, or qubits, in quantum computing and simulations. They could lead to improvements in the operation of quantum computers, which still make too many computation errors to be effective tools, the physicists said.

The problem with quantum computers is that their logic gates — the tools used to perform basic logic functions in computing — "are really bad," Allcock said.

"They fail about 1 percent of the time," he said. "You can do about 100 (operations), then you get garbage out."

Wineland added, "The whole field is in a stage now, because of errors that exist, that we can't do lengthy calculations or simulations of practical value on our machines."

The goal is to get to 10,000 operations without error and then add layers of checks to fix the errors as they happen, he said.

"We want to get to that point," Allcock said. "Then you can use quantum computers for something useful. Right now they're just toys."

Wineland said trapped ions are like a bowl of marbles that have certain magnetic properties. Physicists can apply forces to the ions with different methods, including lasers, Allcock said. But lasers are expensive and complex machines, whereas making logic gates using magnetic forces is cheaper and more practical because they can be generated directly with integrated circuits, he said.

"What we did here is show these techniques work as well as anyone has done logic gates before," he said.

Google and IBM are among the commercial enterprises that have armies of engineers working on such problems, while academic physicists are trying to show there are better, more basic techniques for solving them.

"We've shown you can do it in a technically simpler way," he said.

If physicists and engineers can make quantum computers reliable and able to operate with large enough capacity, they could simulate other systems, Wineland said. For example, a quantum computer could simulate the action of a molecule used in drug therapy without having to synthesize it in a lab.

"There are some very practical, useful outcomes," Wineland said. "We're just scratching the surface."

Quantum computing is based on the principles of quantum theory, which explains the behavior of matter on the atomic and subatomic levels. A quantum bit, or qubit, is the basic unit of information in quantum computing, just as a bit is the basic unit in conventional computing. Unlike a classic bit, which can be 1 or 0, a qubit can be both 1 and 0 at the same time.

Quantum computing has been around since about 1995, when a mathematician at the Massachusetts Institute of Technology named Peter Shor came up with an algorithm using quantum logic ideas that could efficiently break large numbers into a set of simpler equations, a process known as factoring, Wineland said. That was important because most modern encryption algorithms derive their security from the inability to factorize large numbers.

34. 11 important quantum computing industrial revolutionizations

by Madhurjya Chowdhury
https://www.analyticsinsight.net/11-important-quantum-computing-industrial-revolutionizations/

Quantum computing is still very much in infancy, as conventional computing pushes the boundaries of what can be done using known manufacturing methods. Despite this, quantum computing inspires awe in computer scientists, confusion in business leaders, and dread in cryptography specialists. According to some predictions, the quantum computing business will be worth US$5 billion by 2020, indicating that it will grow rapidly in the next few years. So, how can businesses profit from this development? What are the areas where quantum computing excels? Here are 11 quantum computing revolutionaries to look into.

Aviation

Quantum technology has the potential to enable far more sophisticated computer simulations, such as in aviation settings. The time and cost savings associated with assisting in the routing and scheduling of aircraft are considerable. Large businesses such as Airbus and Lockheed Martin are aggressively exploring and investing in the sector in order to take advantage of the technology's computational power and optimization possibilities.

Data Analytics

Quantum computing and quantum mechanics have the ability to solve enormous problems. Due to the data set utilized, topological analysis, an area of study where geometric forms act in certain ways, explains calculations that are just unachievable with today's ordinary computers. This can be reduced to very basic computations using quantum computing.

NASA is exploring using quantum computing to examine the vast amounts of data it collects about the universe and to build better and safer space flight methods.

Forecasting

Large and sophisticated data sets are required for predicting and forecasting diverse scenarios. Traditional weather modeling, for example, has a limit on the number of inputs that can be handled by traditional computers. The model will take longer to finish than the weather forecast if you include too many factors.

Weather affects about 30% of the US GDP in some form, thus being able to anticipate it more correctly would be extremely beneficial to the economy.

Utilities Management

Future supercomputing will have a significant impact on the energy and utility industries. The quantum grid, as well as cybersecurity, load pattern tracking, leakage detection, and consumer and worker analytics, will transform the way billions of people consume electricity and water, as well as how utilities manage these valuable resources. I'm really looking forward to seeing how these things interact.

Cryptography

Advanced cryptography is the most prevalent use of quantum computing. Encryption that employs very big prime number factoring (300+ integers) is impossible to break with today's machines. This decryption might become easy with quantum computers, resulting in far greater protection of our digital lives and possessions. However, we'll be able to crack conventional encryption considerably more quickly as well.

Pattern Matching

Finding patterns in data and utilizing them to forecast future trends is extremely beneficial. Volkswagen is investigating how quantum computing may be used to notify drivers 45 minutes ahead of time of traffic conditions. Quantum computers will make it feasible to match traffic patterns and anticipate the behavior of a system as complicated as today's traffic.

Medical Research

There are literally billions of ways something may respond across the human body, and that number grows exponentially when you think that this could be a medication given to billions of people, each with tiny variations in their genetic makeup.

Today, it might take up to 10 years and billions of dollars for a pharmaceutical company to develop and bring a new medication to market. Quantum computing can substantially reduce costs and time to market, making it easier to reuse pre-approved medicines for new uses, and allow computational chemists to generate new discoveries quicker, perhaps leading to treatments for a variety of ailments.

Supply Chain Management

The supply chain is expected to be the first area where quantum computing will have an influence. If Covid-19 taught us anything, it's that global production networks are inherently complex and risky. Companies will be able to manage supply networks with fewer disruptions because of quantum computing.

Pharmaceutical Research and Development

Quantum computing is based on nonbinary concepts that are more akin to those found in nature. Quantum computers may be faster at creating customized medicines for people with certain genomes, ages, and environments. This natural issue has enough variations to necessitate a new processing model.

Fraud Detection

The next quantum computing revolution has arrived, but we still have a long way to go in understanding what this technology can achieve. Quantum devices ’incredible processing power can push optimizations, random checks, and machine learning to new heights. This implies less risk and greater muscle to identify fraud in finance and cybersecurity. It means better efficiency in assessing patients, handling supply chains, and more across sectors!

Self-Driving Cars

Automakers like Tesla and internet giants like Apple and Google are working on self-driving cars. It will not only raise the level of living for the majority of people, but it will also lower pollution, reduce traffic, and provide a slew of other advantages.

Furthermore, quantum computers are being used by Google and Volkswagen to improve battery, transport, and self-driving technologies. Volkswagen has already improved traffic flow for 10,000 cabs in Beijing, and quantum computing promises much greater benefits.

Conclusion

Quantum computers may be used to convert massive industrial data sets on operational failures into combinatorial problems that, when combined with a quantum-inspired method, can pinpoint which component of a complicated production process led to product failure occurrences. Quantum may assist decrease costly failures in goods like microchips, where the manufacturing process might include thousands of stages. In recent years, billions of dollars have been invested in quantum computing because of its potential to tackle large-scale combinatorics problems quickly and cheaply. The largest potential may be in discovering additional new applications that profit from quantum’s solutions.

35. Cambridge Quantum Computing: Taking The Open Source Route

by Karl Freund
https://www.forbes.com/sites/karlfreund/2021/10/01/cambridge-quantum-computing-taking-the-open-source-route/?sh=7c3bfd382e52

AI has been advancing dramatically in the last decade. It is able to solve classes of problems (facial recognition, machine translation, autonomous vehicles, and others) that were not suitably handled by traditional methods. But there are many important problems that cannot be addressed by traditional or AI approaches, either within a reasonable timeframe or, possibly, at all. Some of these problems can be attacked with Quantum Computing when that technology comes out of research and becomes more widely available.

What is Quantum Computing ?

Quantum Computing presents a radically different approach. Instead of calculating intermediate and final desired values, a quantum computer is configured to represent a problem state. Then, using quantum-mechanical effects such as superposition and entanglement, the quantum circuits suppress the wrong paths and settle very quickly onto the correct answer. If that sounds like black magic to you, you are not alone. Check out this picture of Honeywell's Quantum beast; looks like science fiction!

Quantum computing is already being applied to several challenging problem areas. Cambridge Quantum Computing (CQC) has been working with chemical and pharmaceutical modeling, which has an unmanageably vast solution space. It would take more than the age of the universe to fully analyze these problems with traditional methods, but they become tractable with quantum analysis. Machine learning, finance, and cybersecurity are other promising areas.

Quantum computation is still a new field, with many potential implementation technologies. At least 20 wildly different quantum architectures are being explored, using things like superconducting, trapped ion and photonic. These models all exhibit quantum effects that can be adapted into quantum computer implementations. Obviously, these very different technologies require very different interfaces to configure and "program" them. That provides significant challenges, especially if you want to shift your quantum program onto a different platform.

The TKET Compiler

CQC, which is merging with Honeywell Quantum Solutions, has developed a "quantum compiler" called **TKET**. TKET accepts a high-level specification language, compiles it into an intermediate form that can be optimized, and then maps the result to the desired target architecture.

TKET has several advantages over other quantum compiler implementations:

(i)TKET performs extensive quantum-model optimization on both the logic level and the physical quantum-node implementation level
(ii)As a result of the optimization and other factors, performance ranges from 1 to 3 orders of magnitude better than the other leading quantum compilers
(iii)TKET supports 9 different quantum architectures, vs. 3-5 for its competitors

Dr. Ross Duncan, head of Quantum Software, says they want this to benefit the entire community. "Developers can use TKET for whatever problem they're working on. They can focus on their application itself, instead of worrying about the idiosyncrasies of their particular hardware."

Taking the Open Source route

Earlier this year Cambridge Quantum opened TKET to "open access," granting use licenses to anyone while still retaining full ownership and license to the software. This week CQC completed a year-long process to fully open-source the package. Duncan hopes this will "enable democratization of the quantum community."

There have already been over 100,000 downloads of the package since the open-access release last winter. CQC hopes that momentum, together with TKET's broad feature set and the open-source availability, will help TKET to become a lingua franca for the quantum computing community.

Conclusions

Quantum computing is an exciting new frontier. The technology has the potential to change the face of the industry, and more. We are nowhere near a productization phase, but the major players are making great strides in research and implementation. CQC intends to be a leader in the space.

36. ‘Quantum computer algorithms are linear algebra, probabilities. This is not something that we do a good job of teaching our kids’

by Agam Shah
https://www.theregister.com/2021/10/01/quantum_computing_future/

Let's say, for the sake of argument, that quantum computers will exist in some useful fashion in the not too distant future.

And if that is the case, fundamental changes will be needed in education, supply chains, and national policies for us to use the machines to solve complex problems, panelists said a forum hosted by R Street Institute this week.

"We need ... to prepare people to think about computation in a fundamentally different way," said Chris Fall, senior advisor at the Center for Strategic and International Studies, during the discussion.

On conventional computers, information is encoded in strings of 0s and 1s, while in quantum computers, information is encoded in quantum bits that have a value of 0, 1, or a superposition of both states. This allows quantum computers to store much more information than a classic machine and process it in less time, in theory. There are limitations, such as the fact that they are unstable and prone to error despite efforts to address that, and may hit a wall if unprotected from background radiation. Encryption-breaking quantum computers are forever 15 years away.

Sorry, yes, we're assuming they will eventually work.

Google, D-Wave, IBM, Intel, Microsoft, Honeywell, and so on, are building qubits in different ways. Their goal is to build fault-tolerant machines that can run super-fast calculations by tempering qubit behavior and correcting errors introduced from the environment.

"The routine manipulation of the properties of single atoms in people's devices, devices, cars – that is going to change everything. We don't have a full understanding of how that's going to happen." Fall said.

Starting now, education needs to be better for people to take advantage of the quantum processing breakthroughs as the hardware journey matures, the panelists said. Problem solving and algorithms will look very different in areas like finance and science, for example.

"*The language of quantum algorithms are linear algebra and probabilities. This is not something that we do a good job of teaching our kids from a very early stage. That is kind of where we need to get started now*," Fall said.

Quantum computing is a different problem-solving system and calculates differently from conventional computers, was the gist of the discussion.

Governments will need to drive change if quantum computing is a matter of national interest and public need, said Scott Friedman, a senior policy advisor of the House Homeland Security Committee.

Global legislation to protect semiconductor supply chains, like the CHIPS for America Act and Europe's Chips Act, needs to factor in quantum computing infrastructure, panelists said.

Most cryogenic refrigerators for quantum computers are made in Europe, and the United States needs to work with allies to secure those supply chains, said Allison Schwartz, global government relations and public affairs leader at quantum computer maker D-Wave Systems.

The government also needs to facilitate collaboration and bridge a gap between educators, developers, and scientists involved in algorithms and developing hardware, the panelists said.

The US introduced legislation called QUEST (Quantum User Expansion for Science and Technology) for increased access of quantum hardware and resources for research and further education. A National Quantum Initiative Act (NQI) was signed into law in 2018 to supercharge quantum computing development and research, but activity around these have stalled.

"The advisory committee for the NQI hasn't met in a while ... on the executive branch side. An easy next step to bring more focus in this area would be to convene that again and get broader input from the community," said Kate Weber, policy lead for quantum, robotics, and fundamental research at Google, which hopes to a build a fault-tolerant computer by 2030.

The moderator, R Street Institute senior fellow Miles Taylor, raised the idea of quantum computers creating sentient beings, much like the machines in the Terminator movies.

"I don't know if we're going to have a sentient computer," CSIS's Fall said, adding, "we're learning to manipulate single atoms at ... industrial scale. That's not a laboratory project. It'll change the world."