Crypto News

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

January 01, 2022

Editorial

SEATTLE, WA – January, 1st, 2022. Happy New Year! Here's the first Crypto News edition of 2022! Want a recap of the biggest data breaches and hacks of 2021? Scroll down to article #1 and get a breakdown month by month along with interesting facts. For example, did you know that the record for the largest insurance payout was set in 2021 for $40 million? Wow! I prefer to stay on the white hat side but it seems to me that black hats are doing rather well for themselves these days. Are you into cars? Take a look at article #2 which talks about using quantum computers on cars like the BMW in the near future. How amazing is that? But it's not just BMW, it's companies like Thales, Airbus, PayPal, and LG who see the potential of quantum computers and their uses in their respective industries. You can also scroll down to article #40 which unveils the winners of the BMW Group Quantum Computing Challenge. It's exciting to see so many industry leaders recognizing the value of quantum computing. Next, go ahead and be a "cool kid" and learn about qutrits. Yes, you read that right, it's "qutrit". The term signifies a third energy state that's been added to Rigetti's qubits. Learn how they plan to leverage this third state in their qutrits by reading article #17. Last but not least, take a look at article #51. Stanford researchers have proposed a design for a photonic quantum computer. The best part? This technology uses a few pieces of equipment that are commercially available and being upgraded often since they are used in other large industries. This is definitely something to keep your eye on. There's a number of other interesting articles in this month's newsletter that you won't want to miss. Happy reading!

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

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

1.The biggest data breaches, hacks of 2021

by Charlie Osborne
https://www.zdnet.com/article/the-biggest-data-breaches-of-2021/

In 2021, thousands of new cybersecurity incidents have been recorded -- and while cryptocurrency theft and data loss are now commonplace, this year stands out due to several high-profile incidents involving ransomware, supply chain attacks, and the exploitation of critical vulnerabilities.

The Identity Theft Research Center (ITRC) has reported an increase of 17% in the number of recorded data breaches during 2021 in comparison to 2020. However, an entrenched lack of trans-

parency around the disclosure of security incidents continues to persist -- and so this may be a low ball estimation.

According to IBM, the average cost of a data breach has now reached over $4 million, while Mimecast estimates that the average ransomware demand levied against US companies is well over $6 million. The world record for the largest payout, made by an insurance company this year, now stands at $40 million.

Experts have warned that the security issue could persist for years with the recent emergence and rapid exploitation of the Log4j vulnerability. That goes for data leaks, breaches, and theft, too, which are unlikely to decline in number in the near future.

Here are some of the most notable security incidents, cyberattacks, and data breaches over 2021.

January:

- **Livecoin:** Following an alleged hack in December, cryptocurrency exchange Livecoin slammed its doors shut and exited the market in January. The Russian trading post claimed that threat actors were able to break in and tamper with cryptocurrency exchange rate values, leading to irreparable financial damage.

- **Microsoft Exchange Server**: One of the most damaging cybersecurity incidents this year was the widespread compromise of Microsoft Exchange servers caused by a set of zero-day vulnerabilities known collectively as ProxyLogon. The Redmond giant became aware of the flaws in January and released emergency patches in March; however, the Hafnium state-sponsored threat group was joined by others for months after in attacks against unpatched systems. Tens of thousands of organizations are believed to have been compromised.

- **MeetMindful**: The data of over two million users of the dating app was reportedly stolen and leaked by a hacking group. The information leaked included everything from full names to Facebook account tokens.

February:

- **SITA**: An IT supplier for aviation services around the world, SITA, said a security incident involving SITA Passenger Service System servers led to the exposure of personal, identifiable information belonging to airline passengers. Airlines involved in the data breach were then required to reach out to their customers.

- **ATFS**: A ransomware attack against payment processor ATFS forced multiple US cities to send out data breach notifications. The cybercriminal group which claimed responsibility, Cuba, claimed to have stolen a wide range of financial information on their leak site.

March:

- **Mimecast:** Due to the Solarwinds supply chain attack disclosed in December 2020, Mimecast found itself as a recipient of a malicious software update that compromised the firm's systems. Mimecast said that its production grid environment had been compromised, leading to the exposure and theft of source code repositories. In addition, Mimecast-issued certificates and some customer server connection datasets were also caught in the breach.

- **Tether**: Tether faced an extortion demand from cyberattackers who threatened to leak documents online that would "harm the Bitcoin ecosystem." The demand, of approximately $24 million or 500 Bitcoin (BTC), was met with deaf ears as the blockchain organization refused to pay.

- **CNA Financial**: CNA Financial employees were left unable to access corporate resources and were locked out following a ransomware attack which also involved the theft of company data. The company reportedly paid a $40 million ransom.

April:

- **Facebook**: A data dump of information belonging to over 550 million Facebook users was published online. Facebook IDs, names, dates of birth, genders, locations, and relationship statuses were included in the logs, of which Facebook -- now known as Meta -- said was collected via scraping in 2019.

May:

- **Colonial Pipeline**: If there was ever an example of how a cyberattack can impact the physical world, the cyberattack experienced by Colonial Pipeline is it. The fuel pipeline operator was struck by ransomware, courtesy of DarkSide, leading to fuel delivery disruption and panic buying across the United States. The company paid a ransom, but the damage was already done.

- **Omiai**: The Japanese dating app said unauthorized entry may have led to the exposure of data belonging to 1.7 million users.

June:

- **Volkswagen, Audi:** The automakers disclosed a data breach impacting over 3.3 million customers and some prospective buyers, the majority of which were based in the United States. A finger was pointed at an associated vendor as the cause of the breach, believed to be responsible for exposing this data in an unsecured manner at "some point" between August 2019 and May 2021.

- **JBS USA:** The international meatpacking giant suffered a ransomware attack, attributed to the REvil ransomware group, which had such a disastrous impact on operations that the

company chose to pay an $11 million ransom in return for a decryption key to restore access to its systems.

July:

- **UC San Diego Health**: UC San Diego Health said employee email accounts were compromised by threat actors, leading to a wider incident in which patient, student, and employee data potentially including medical records, claims information, prescriptions, treatments, Social Security numbers, and more were exposed.

- **Guntrader.uk**: The UK trading website for shotguns, rifles, and shooting equipment said that records belonging to roughly 100,000 gun owners, including their names and addresses, had been published online. As gun ownership and supply are strictly controlled in the UK, this leak has caused serious privacy and personal safety concerns.

- **Kaseya**: A vulnerability in a platform developed by IT services provider Kaseya was exploited in order to hit an estimated 800 - 1500 customers, including MSPs.

August:

- **T-Mobile:** T-Mobile experienced a yet-another data breach in August. According to reports, the names, addresses, Social Security numbers, driver's licenses, IMEI and IMSI numbers, and ID information of customers were compromised. It is possible that approximately 50 million existing and prospective customers were impacted. A 21-year-old took responsibility for the hack and claimed to have stolen roughly 106GB of data from the telecoms giant.

- **Poly Network**: Blockchain organization Poly Network disclosed an Ethereum smart contract hack used to steal in excess of $600 million in various cryptocurrencies.

- **Liquid**: Over $97 million in cryptocurrency was stolen from the Japanese cryptocurrency exchange.

September:

- **Cream Finance**: Decentralized finance (DeFi) organization Cream Finance reported a loss of $34 million after a vulnerability was exploited in the project's market system.

- **AP-HP**: Paris' public hospital system, AP-HP, was targeted by cyberattackers who managed to swipe the PII of individuals who took COVID-19 tests in 2020.

- **Debt-IN Consultants**: The South African debt recovery firm said a cyberattack had resulted in a "significant" incident impacting client and employee information. PII, including names, contact details, salary and employment records, and debts owed, are suspected of being involved.

October:

- **Coinbase:** Coinbase sent out a letter to roughly 6,000 users after detecting a "third-party campaign to gain unauthorized access to the accounts of Coinbase customers and move customer funds off the Coinbase platform." Cryptocurrency was taken without permission from some user accounts.

- **Neiman Marcus:** In October, Neiman Marcus made a data breach that occurred in May 2020 public. The intrusion was only detected in September 2021 and included the exposure and potential theft of over 3.1 million payment cards belonging to customers, although most are believed to be invalid or expired.

- **Argentina:** A hacker claimed to have compromised the Argentinian government's National Registry of Persons, thereby stealing the data of 45 million residents. The government has denied the report.

November:

- **Panasonic:** The Japanese tech giant revealed a cyberattack had taken place -- a data breach occurring from June 22 to November 3, with discovery on November 11 -- and admitted that information had been accessed on a file server.

- **Squid Game:** The operators of a cryptocurrency jumping on the popularity of the Netflix show Squid Game (although not officially associated) crashed the value of the SQUID token in what appears to be an exit scam. The value plummeted from a peak of $2,850 to $0.003028 overnight, losing investors millions of dollars. An anti-dumping mechanism ensured that investors could not sell their tokens -- and could only watch in horror as the value of the coin was destroyed.

- **Robinhood:** Robinhood disclosed a data breach impacting roughly five million users of the trading app. Email addresses, names, phone numbers, and more were accessed via a customer support system.

December:

- **Bitmart:** In December, Bitmart said a security breach permitted cyberattackers to steal roughly $150 million in cryptocurrency and has caused total losses, including damages, to reach $200 million.

- **Log4j:** A zero-day vulnerability in the Log4j Java library, a remote code execution (RCE) flaw, is now being actively exploited in the wild. The bug is known as Log4Shell and is now being weaponized by botnets, including Mirai.

- **Kronos**: Kronos, an HR platform, became a victim of a ransomware attack. Some users of Kronos Private Cloud are now facing an outage that may last weeks -- and just ahead of Christmas, too.

2.Quantum computers are on the path to solving bigger problems for BMW, LG and others

by Stephen Shankland
https://www.cnet.com/tech/computing/quantum-computers-will-help-solve-bigger-problems-in-2022/

After years of development, quantum computers reached a level of sophistication in 2021 that emboldened commercial customers to begin dabbling with the radical new machines. Next year, the business world may be ready to embrace them more enthusiastically.

BMW is among the manufacturing giants that sees the promise of the machines, which capitalize on the physics of the ultrasmall to soar over some limits of conventional computers. Earlier this month, the German auto giant chose four winners in a contest it hosted with Amazon to spotlight ways the new technology could help the automaker.

The carmaker found quantum computers have potential to optimize the placement of sensors on cars, predict metal deformation patterns and employ AI in quality checks.

"We at the BMW Group are convinced that future technologies such as quantum computing have the potential to make our products more desirable and sustainable," Peter Lehnert, who leads BMW's research group, said in a statement.

For years, researchers worked on quantum computers as more or less conceptual projects that take advantage of qubits, data processing elements that can hold more than the two states that are handled by transistors found in conventional computers. Even as they improved, quantum computers were best suited for research projects, some as basic as figuring out how to program the exotic machines. But at the current rate of progress, they'll soon become powerful enough to tackle computing jobs out of reach of conventional computers.

Like cloud computing before it, quantum computing will be a service that most corporations rent from other companies. The rigs require constant attention and are notoriously fiddly. Though more work is required to tap their full potential, quantum computers are becoming more and more stable, a development that's helping corporations overcome initial hesitance.

Georges-Olivier Reymond, chief executive of startup Pasqal, says the progress is turning around skeptics who previously viewed quantum computing as a fantasy. A few years ago, employees at large corporations would roll their eyes when he brought up the subject, but that's changed, Reymond says.

"Now each time I talk to them I have a positive answer," Reymond said. "They are ready to engage."

One new customer is European defense contractor Thales, which is interested in quantum computing applications in sensors and communications. "Pasqal's quantum processors can efficiently address large size problems that are completely out of reach of classical computing systems," Thales Chief Technology Officer Bernhard Quendt said in a statement.

BMW isn't alone in its determination to evaluate the practical application of quantum computers. Aerospace giant Airbus, financial services company PayPal and consumer electronics maker LG Electronics are among the commercial businesses looking to use the machines to refine materials science, streamline logistics and monitor payments.

Of course, quantum computing is still a tiny fraction of the traditional computing market, but it's growing fast. About $490 million was spent on quantum computers, software and services in 2021, Hyperion Research analyst Bob Sorensen said at the Q2B conference held by quantum computing software company QC Ware in December. He expects spending to grow by 22% to $597 million in 2022 and at an average of 26% a year through 2024. By comparison, spending on conventional computing is expected to rise 4% in 2021 to $3.8 trillion, Gartner analysts predict.

The growing commercial activity is notable given that using a quantum computer costs $3,000 to $5,000 per hour, according to Jean-Francois Bobier, an analyst at Boston Consulting Group. A conventional, high-performance computer hosted on a cloud service costs a half penny for the same amount of time.

Analysts say the real spending on quantum computing will start when the industry tackles error correction, a solution to the vexing problem of easily perturbed qubits that derail calculations. The fidelity of a single computing step on the most advanced machines is around 99.9%, leaving a degree of flakiness that makes a raw quantum computing calculation unreliable. As a result, quantum computers have to run the same calculation many times to provide confidence that the answer is correct.

Once error correction is mature, the revenue generated through quantum computing will explode, according to Boston Consulting Group. With today's machines, that value will likely total between $5 billion and $10 billion by 2025, according to the consultancy's estimates. Once error corrected machines arrive, the total could leap forward to hit $450 billion to $850 billion by 2040.

Software and services that hide the complexity of quantum computers also will boost usage. IonQ CEO Peter Chapman predicts that in 2022, developers will be able to easily train their AI models with quantum computers. "You don't need to know anything about quantum," Chapman said. "You just give it the data set and it spits back a model."

Among the signs of commercial interest:

- Carmaker Daimler and oil giant ExxonMobil have contracted with IBM, an early proponent of quantum computing, to use some of the tech company's 22 machines. (Big Blue will soon be adding Eagle, a new, more powerful device that uses a 127-qubit processor.) The companies

are prime candidates for the materials science breakthroughs that quantum computers could someday deliver. They could also use the machines for help with logistics challenges like getting the right equipment in the field when it's needed or the proper components to the factory in time for manufacturing.

- Airbus, LG Electronics, health care company Johnson & Johnson, energy company EDF and chemicals giant BASF are among the industrial enterprises jockeying for time on Pasqal's single quantum computer. The startup is working on a relatively new "neutral atom" design that uses lasers to carefully arrange rubidium atoms then use them as qubits to process data. Many quantum computing startups are in the US, but Pasqal, with headquarters in France, benefits from European customers and government programs.

- PayPal is testing a quantum annealer, a type of quantum computer suited for solving optimization problems and made by D-Wave Systems, to guide its fraud-detection work, according to Vidyut Naware, the company's director of AI research. He also told the Q2B crowd that PayPal is running the test to get a better idea of how quantum computing can be deployed more effectively.

- Amazon Web Services offers customers access to machines from IonQ, Rigetti Computing and D-Wave Systems. It'll soon be adding machines from QuEra and Oxford Quantum Circuits, and is building its own quantum machine. Among those using its services are JPMorgan Chase, which is testing it for optimization work, like managing its clients' investment portfolios.

- Microsoft is working on its own quantum computing approach, called a topological qubit design. The work isn't commercially available yet but Microsoft's Azure cloud service offers access to quantum computers and to quantum computer simulators that are an important stepping stone. The company has also struck a deal with KPMG to help customers test the quantum computing water using Azure.

- Quantinuum, the company formed when hardware maker Honeywell Quantum Solutions merged with software maker Cambridge Quantum, launched a service in December to generate random numbers. That may sound obscure, but such numbers are a foundation for modern encryption. Among those trying the service are Fujitsu and Axiom Space.

- Quantum chemistry software startup Qunasys offers software to customers like Mitsubishi Chemical Corporation, said CEO Tennin Yan. Quantum chemistry and materials science could help engineers find better solar panel materials, electric vehicle batteries and plastics.

Quantum computers today are more of a luxury than a necessity. But with their potential to transform materials science, shipping, financial services and product design, it's not a surprise companies like BMW are investing. The automaker stands to benefit from knowing better how materials will deform in a crash or training its vehicles' vision AI faster. Though quantum computers might not produce a payoff this year or next, there's a cost to missing out on the technology once it matures.

3.Army Sets Up New Quantum Computing Lab, Artificial Intelligence Centre

by PTI
https://www.ndtv.com/india-news/army-sets-up-new-quantum-computing-lab-artificial-intelligence-centre-in-mhow-2677938

The Army has set up a quantum computing laboratory and a centre for artificial intelligence (AI) at a military engineering institute in Madhya Pradesh's Mhow.

The two centres will carry out extensive research in developing transformative technologies for use by the armed forces.

"The Army, with support from the National Security Council Secretariat (NSCS), has recently established the Quantum Lab at Military College of Telecommunication Engineering, Mhow to spearhead research and training in this key developing field," the Defence Ministry said.

It said the Indian Army is making steady and significant strides in the field of emerging technologies.

Chief of Army Staff General MM Naravane visited the facility during his recent visit to Mhow.

"Indian Army has also established an Artificial Intelligence (AI) Centre at the same institution with over 140 deployments in forward areas and active support of industry and academia," the ministry said in a statement.

"Training on cyber warfare is being imparted through a state-of-the-art cyber range and cyber security labs," it said.

The ministry said the research undertaken by the Army in the field of quantum technology will help it leapfrog into the next generation of communication and transform the current system of cryptography to post-quantum cryptography.

It said the key thrust areas are quantum key distribution, quantum communication and quantum computing, among others.

4.Year End Commentary Series Quantinuum on The State of Quantum

by Dan O'Shea
https://www.insidequantumtechnology.com/news-archive/year-end-commentary-series-quantinuum-on-the-state-of-quantum-2/

As we wrap up 2021 and begin 2022, IQT News is asking executives from several companies across the quantum sector to weigh in on the state of the industry, key challenges that remain and visions and hopes of the future.

The latest entry in this series comes from Tony Uttley, president of Quantinuum. Almost no company in the quantum space had a more eventful 2021 than Quantinuum, which did not even exist until late in the year. The new firm is the result of the merger between Honeywell Quantum Solutions and Cambridge Quantum, which was announced earlier in the year. Prior to that deal, Honeywell and Cambridge Quantum each were making a big splash on their own, Honeywell with its H Series quantum processor and Cambridge Quantum with numerous software announcements, including the open source availability of its TKET hardware-agnostic software development kit and the launch of its Quantum Natural Language Processing toolkit. After the merger was completed and Quantinuum came to life, the company earlier this month announced its Quantum Origin cryptographic key platform.

Here's Uttley on the sector's accomplishments this year, and what next year could bring:

2021 saw the continuation, and in fact an acceleration, of a trend that now goes back at least two if not three years where significant milestones are reached on a variety of areas of quantum computing, ranging from hardware to control systems, to error correction, to middleware and operating systems, to applications.

- Several organizations who have been known to be working on the manufacturing of quantum computers but who had not yet provided any details of their devices, released new quantum processors.
- In addition, several larger groups who have existing processors unveiled upgrades or new processors that matched those organization's predicted performance gains. In many respects, this maintained the trend of exponential increases in quantum processor capability.
- With the roll-out of sophisticated open-source software and the expansion of platform-inclusive approaches, the community of people and organizations participating in quantum computing increased dramatically.
- There has recently been a notable shift away from purely nationalistic commitments by countries towards an approach where countries began to express interest in joint coopera-

tion within the field of quantum computing. A prime example occurred in early November, when the governments of the United Kingdom and the United States released a joint statement to enhance cooperation in the area of quantum information science and technology.

- Importantly, multiple organizations demonstrated advances in quantum error correction, including a demonstration of real-time quantum error correction by Quantinuum which marks a huge advance towards fault tolerant devices.

- Perhaps most importantly we saw, for the first time, a broadly available and commercially relevant product that could only be created using today's quantum computers.

2022 is starting in a very different place than 2021. With more resources (both money and people) now focused on making near-term quantum computing relevant, there is an increasing likelihood that we will see further gains within the year. Remember all the advances that have been announced in 2021 and 2020 were the result of sustained investment and resource allocation in the previous years. Given the exponential increase in resources we can expect 2022 to show a similar trend in hardware, including new entrants, middleware and applications.

5.D-Wave opens up to gate-model quantum computing

by Jack Vaughan
https://venturebeat.com/2021/12/28/d-wave-opens-up-to-gate-model-quantum-computing/

Recent advances in quantum computing show progress, but not enough to live up to years of hyperbole. An emerging view suggests the much-publicized quest for more quantum qubits and quantum supremacy may be overshadowed by a more sensible quest to make practical use of the qubits we have now.

The latter view holds particularly true at D-Wave Systems Inc., the Vancouver, B.C., Canada-based quantum computing pioneer that recently disclosed its roadmap for work on logic gate-model quantum computing systems.

D-Wave's embrace of gates is notable. To date, the company focuses solely on quantum annealing processors. Using this probabilistic approach, it has achieved superconducting qubit processor counts that it claims outpaces most others. Its latest Advantage system boasts 5,000 qubits. That's well ahead of the 127-qubit device IBM reported in November.

There is an important caveat, as followers of the quantum business know. D-Wave's annealing qubits don't have the general quantum qualities that competitive quantum gate-model systems have, and the degree of processing speed-up they provide has been questioned.

Questions arise despite placing its systems in research labs at Google, NASA, Los Alamos National Laboratory, and elsewhere. D-Wave's qubit counts have been faulted by critics for specializing in a purpose-built approach aimed at a certain class of optimization problems.

Bring on the NISQ

Still, the company has a leg-up with its experience compared to most competitors, having fabricated and programmed superconducting parts since at least 2011.

For that matter, the gate-model quantum computing crew's benchmarks have come under attack, too, and its battles with scaling and quantum error (or "noise") correction have spawned the term "noisy intermediate-scale quantum" (or "NISQ") to describe the present era, where users have to begin to do what they can with whatever working qubits they have.

While it will continue to work on its annealing-specific quantum variety, D-Wave has joined a gate-model quantum competition where there appears plenty of room for growth. According to Statistica, the revenues for global quantum computing in 2020 equaled $412 million, but is predicted to jump to $8.6 billion in 2027.

Bread, butter, and quantum computing

As it moves to broaden its product mix, D-Wave hopes to boost its current system sales and availability too. News of its roadmap was followed by the word that NEC Corp. would become the first global reseller of D-Wave's Leap quantum cloud service. D-Wave also launched a Quantum QuickStart kit that echoes competitors' efforts to open-up quantum programming to everyday Python developers via the cloud.

The original decision on quantum annealing has proven itself, said Mark Johnson, vice president for quantum technology and systems products at D-Wave. He cited the use of D-Wave systems in solving optimization scheduling and routing problems while discussing D-Wave's new roadmap with Venture Beat.

Johnson said the practical potential of quantum annealing was among the factors that led him to join the company in the early 2000s, after work on superconducting circuits at defense contractor TRW (now part of Northrop Grumman).

"Today, it's the most effective sort of quantum technology for solving problems. There is a natural error tolerance to quantum annealing," he said. Still, competitive gate-level advances continue.

"We're now learning just in the last three or four years, from a growing body of published theoretical work, that it is unlikely quantum annealing is always going to be better than gate models at optimization problems," Johnson said.

That said, error correction is clearly a concern. But, Johnson suggests this is a good time to join the quest to solve that as an industry. "We will all figure out together how to go beyond that," he said. That is, while still pursuing annealing advances.

"Our bread and butter is going to continue to be quantum annealing, but we are adding another product line," he said. D-Wave is also at work on quantum-classical hybrid solvers for optimization, he noted, to combine classical enterprise computing with quantum resources.

Accelerators fill the gap

D-Wave's expansion to include gate models is a natural progression for a company that "cut its teeth on annealing architecture," according to Bob Sorensen, senior vice president, and chief analyst for quantum computing at Hyperion Research.

"The company has good skills in building cryogenically cooled technology usable for quantum computing applications," he said. "In the transition to a gate-model architecture — although it's not trivial — they bring a lot of smarts to the table."

At the same time, the ongoing movement that sees quantum processing becoming a part of established computing stacks is the important one to watch, Sorensen said. It's not unfair to call this a hybrid approach, he said.

"Parts of a job might be done on the one system, go over to the other, and then come together – iterating between the classical and the quantum system to take advantage of the performance capabilities of both," Sorensen said.

Likely, he said, quantum computing will offer benefits for workloads in specific applications. As such, quantum processors in hybrid quantum-classical combos will resemble the GPU in the role it's assumed for AI in datacenters; that is: as an auxiliary processor.

"Think of it as an accelerator for specific advanced computing workloads," he said.

Effectively handling workloads is more important than reaching a 1,000 qubit gate-model level, or proving quantum supremacy versus classical computing. Instead, what is important for vendors, "is demonstrating the fact that you can solve end-user problems effectively," Sorensen said.

6.Indian scientists devise technique for more efficient quantum computing

by IANS
https://www.daijiworld.com/news/newsDisplay?newsID=909189

Correlations between waves in atomic systems or spin coherences are long-lived at ultralow temperatures, says a new study by scientists who have developed a new technique to measure it as a system with long-lived spin coherences is a better resource as a quantum computer.

This is because it allows quantum operations and logic gates to be more efficiently implemented so that the system becomes a better quantum sensor compared to systems where coherence is short-lived, a Science and Technology Ministry release said.

This newly explored property of atomic systems at low temperature can be exploited for efficient quantum sensing and quantum information processing for application in quantum computation and secure communication, it said. "The newly discovered technique can help study the real-time dynamics of quantum phenomena such as quantum phase transitions in a non-invasive manner."

Spin is a fundamental quantum property of atoms and elementary particles such as electrons and protons. As atoms are cooled to lower temperatures, their quantum nature is manifested more prominently. However, while the spin degree of freedom is a highly discussed topic, especially in the context of quantum information processing, the dynamical measurements on spins at ultralow temperatures were not available. This is because most of the detection techniques in cold atom experiments are destructive and disturbs the atomic sample during detection.

A team of scientists from the Raman Research Institute (RRI), Bengaluru, an autonomous institute of the Department of Science & Technology, have measured the spin properties of atoms cooled to micro-Kelvin temperatures using the new method they have devised.

Quantum properties dominate over everyday classical observations at this temperature -- very near absolute zero temperature, and it is for the first time that spin dynamics have been detected at this temperature regime.

With the new technique, the scientists measured the properties of spins and lifetime of an atomic spin state with a million-fold improvement in detection sensitivity compared to the existing technology. They proved that spin coherence at this low temperature is long-lived.

In this work, led by Sanjukta Roy, Dibyendu Roy, and Saptarishi Chaudhuri and co-authored by Ph.D. students Maheswar Swar and Subhajit Bhar from RRI, the researchers increased signal strength of spin noise by a million-fold by using coherent laser drive. They made the spin noise spectroscopy technique usable for spectroscopists measuring systems where signal level is too low to detect. The research has been published in the journal Physics Review Research. The work has been financially supported by funding from the Department of Science and Technology and Ministry of Electronics and Information Technology.

According to the RRI team, this work derives its original motivation from Nobel laureate Sir C.V. Raman's seminal work on light scattering.

According to the team, this technology can be used to make devices that can precisely detect small magnetic fields, which has important applications in mining and prospecting. The work also has important applications in biomedical imaging, where time-resolved measurements of small magnetic fields are required.

7.We Encrypted the Web: 2021 Year in Review

by Alexis Hancock
https://www.eff.org/deeplinks/2021/12/we-encrypted-web-2021-year-review

In 2010, EFF launched its campaign to encrypt the entire web—that is, move all websites from non-secure HTTP to the more secure HTTPS protocol. Over 10 years later, 2021 has brought us even closer to achieving that goal. With various measurement sources reporting over 90% of web traffic encrypted, 2021 saw major browsers deploy key features to put HTTPS first. Thanks to Let's Encrypt and EFF's own Certbot, HTTPS deployment has become ubiquitous on the web.

Default HTTPS in All Browsers

For more than 10 years, EFF's HTTPS Everywhere browser extension has provided a much-needed service to users: encrypting their browser communications with websites and making sure they benefit from the protection of HTTPS wherever possible. Since we started offering HTTPS Everywhere, the battle to encrypt the web has made leaps and bounds: what was once a challenging technical argument is now a mainstream standard offered on most web pages. Now HTTPS is truly just about everywhere, thanks to the work of organizations like Let's Encrypt. We're proud of EFF's own Certbot tool, which is Let's Encrypt's software complement that helps web administrators automate HTTPS for free.

The goal of HTTPS Everywhere was always to become redundant. That would mean we'd achieved our larger goal: a world where HTTPS is so broadly available and accessible that users no longer need an extra browser extension to get it. Now that world is closer than ever, with mainstream browsers offering native support for an HTTPS-only mode.

In 2020, Firefox announced an "HTTPS-only" mode feature that all users can turn on, signaling that HTTPS adoption was substantial enough to implement such a feature. 2021 was the year the other major browsers followed suit, starting with Chrome introducing an HTTPS default for navigation when a user types in the name of a URL without specifying insecure HTTP or secure HTTPS. Then in June, Microsoft's Edge announced an "automatic HTTPS feature" that users can opt into. Then later in July, Chrome announced their "HTTPS-first mode", which attempts to automatically upgrade all pages to HTTPS or display a warning if HTTPS isn't available. Given Chrome's dominant share of the browser market, this was a huge step forward in web security. Safari 15 also implemented a HTTPS-first mode in its browsers. However, it does not block insecure requests like in Firefox, Chrome, and Edge.

With these features rolled out, HTTPS is truly everywhere, accomplishing the long-standing goal to encrypt the web.

SSL/TLS Libraries Get A Critical Update

SSL/TLS libraries are heavily used in everyday critical components of our security infrastructure, like transportation of web traffic. These tools are primarily built in the C programming language. However, C has a long history of memory safety vulnerabilities. So the Internet Security Research Group has led the development of building an alternative to certain libraries like OpenSSL in the Rust language. Rust is a modern, memory-safe programming language and the TLS library built in Rust has been named "Rustls." Rustls has also been integrated for support in popular networking command line utilities such as Curl. With Rustls, important tools that use TLS can gain memory safety and make networks ever more secure and less vulnerable.

Making Certbot More Accessible

Since 2015, EFF's Certbot tool has helped millions of web servers deploy HTTPS by making the certificate process free and easy. This year we significantly updated the user experience of Cerbot's command-line output for clarity. We also translated parts of the website into Farsi in response to user requests, and now we have the Instructions Generator available in this language. We hope to add more languages in the future and make TLS deployment in websites even more accessible across the globe.

On The Horizon

Even as we see positive movement by major browsers—from the HTTPS-by-default victories above to ending insecure FTP support and even Chrome adopting a Root Store program—we are also watching the potential dangers to these gains. Encrypting the net means sustaining the wins and fighting for tighter controls across all devices and major services.

HTTPS is ubiquitous on the web in 2021, and this victory is the result of over a decade of work by EFF, our partners, and the supporters who have believed in the dream of encrypting the web every step of the way.

8.Quantum and the Future of Cryptography

by Vidya Subramanian
https://www.nationaldefensemagazine.org/articles/2021/12/27/quantum-and-the-future-of-cryptography

The ability to encrypt information is an essential part of military command and control, just as breaking military codes has been a decisive factor in modern warfare. With that in mind, the United States should take steps now to prepare for a day when adversaries could have quantum computing-enabled decryption capabilities.

Examples of successful codebreaking abound, from the deciphering of the Zimmermann Telegram that brought the United States into World War I to the cracking of Japanese codes that led to victory at the Battle of Midway. Most famously, cracking the Enigma code helped change the course of World War II. Though still an essential element of military command and control, cryptography also underpins security across all segments of our economy, including phone calls, credit card payments, banking transactions and most web searches.

Ensuring that data is successfully encrypted and thus inaccessible to attackers is key to maintaining a strong cyber defense posture. To that end, cryptographic technologies are widely employed to authenticate sources, protect stored information, and share data in a confidential and secure manner. Algorithms currently in use are so advanced and have revolutionized data security to such an extent that even the fastest classical computers could take years, in some cases decades, to unlock encrypted files. As a result, rather than attempt brute force decryption, hackers have instead preferred to steal encryption keys or find weak links in a security network to bypass secure channels and steal decrypted data.

For example, in the recent Colonial Pipeline incident, attackers obtained access to the IT system through a legacy Virtual Private Network, or VPN, profile that had not been used or monitored for years. Better enforcement of cyber hygiene is a short-term solution, but in the long-term, security networks must also be overhauled to implement cryptographic algorithms designed to fend off future attacks made possible with emerging technologies such as quantum computing.

For decades now, quantum computing has been hailed as one of the next big revolutions. Quantum computing is not just faster than traditional computing methods, but a fundamentally different approach to solve seemingly intractable problems. The mathematical operations that most traditional cryptographic algorithms rely on could be cracked with a sufficiently strong quantum computer.

With the potential that quantum could have on the international economy, it is no surprise that billions of dollars are being invested to fund research in this emerging technology area. In the United States, efforts are being led by academia, government labs and technology companies across the industrial base. However, China is investing heavily and is close behind. President Xi Jinping's government has spent more than $10 billion to set up the National Laboratory for Quantum Information Sciences, and at the current rate will spend more on quantum research than any other nation by 2030.

Practical quantum computers are still a long way off. The design and operation of an operational quantum computer, let alone programming it, will be exceptionally challenging.

Traditional computers use bits that can hold only one of two values — 0 or 1. But a quantum computer employs quantum-bits, also known as qubits, that can be both 0 and 1 at the same time, thus giving the computer its exceptional power. However, these qubits are also fragile, and interactions with their surroundings can distort them. Existing quantum computers have been built with only a few handfuls of qubits, while a usable quantum computer would require something closer to a million high-quality qubits with robust error correction.

Larger computations would also require bigger quantum chips with many millions of connections. Even if that were possible, we do not currently have the capability to control multiple qubits on the time scales required for useful operations, on the order of tens of nanoseconds.

Notably, only a limited set of problems have been identified that can currently be solved more effectively on a quantum computer than a traditional one.

However, given the pace of advancement and magnitude of investments by peer competitors, we should not wait to implement quantum-resistant algorithms on our security networks. There are steps we can take now to guard against future quantum computational capabilities, including the implementation of post-quantum cryptography algorithms that are secure against both classical and quantum computers. Of course, systems protected by even the most robust quantum-resilient algorithms would still be vulnerable to attack via weak links in a network, so these are necessary but not sufficient steps.

In 2015, the National Security Agency announced plans to transition to a quantum-resistant cipher suite and encouraged partners and vendors to do the same. The National Institute of Standards and Technology established the Post-Quantum Cryptography Standardization program and competition in 2016, to upgrade public key encryption to a quantum-proof model. Schemes submitted were analyzed internally to standardize the best ones for use in products and services. Three signature schemes were selected as finalists in Round 3 in July 2020, with some alternate schemes considered for further analysis. NIST also plans to publish a playbook to guide government and industry through the transition of their crypto systems to quantum-resilience.

It would be difficult to predict when, or even if, quantum computing will provide our adversaries, or even bad actors, with the ability to creak previously unbreakable codes. But regardless of the timeline for that threat, we can take steps today that will significantly reduce the potential risks posed by that future capability.

9.How fast can quantum computers process information? - study

by Jerusalem Post Staff
https://www.jpost.com/science/article-689720

A new peer-reviewed study by physicists at the University of Bonn in Germany and the Technion - Israel Institute of Technology examines which factors determine the speed at which calculations can be performed by a quantum computer. The study draws on previous research by Soviet physicists Leonid Mandelstam and Igor Tamm.

Quantum computers, unlike their conventional counterparts, use quantum mechanics to process information, which enables them to solve a wider range of problems - but still, there are limits.

Conventional computers use binary code composed of sequences of 1s and 0s known as "bits" to store information, whereas quantum computers use quantum bits. Also known as "qubits," these units of information "resemble a wave rather than a series of discrete values," according to the Technion.

Information is linked together in conventional computers by building blocks known as "gates," and when gates are combined, simple calculations may be performed. In quantum computers, information processing occurs in a similar manner where "gates change the wave function."

Dr. Andrea Alberti of the Institute of Applied Physics at the University of Bonn and one of the study's authors explained that "They require a minimum amount of time to transform the wave function and the information this contains." Mandelstam and Tamm theoretically deduced this required minimum time in their research, and this new study investigates the limit they determined.

To investigate that limit, this study's authors initially observed the motion of cesium atoms as they rolled "like marbles" down a light bowl, though this method proved to have variables that hindered the researchers' ability to identify information changes. "We therefore devised a different method to detect the deviation from the initial state," Alberti explained.

Another strategy was then attempted. Gal Ness, a doctoral student at the Technion and the lead author of the study explained that the team "used fast light pulses to create a so-called quantum superposition of two states of the atom. Figuratively speaking, the atom behaves as if it had two different colors at the same time." Each copy of the atom "takes a different position in the light bowl: One is high up on the edge and 'rolls' down from there. The other, conversely, is already at the bottom of the bowl. This twin does not move - after all, it cannot roll up the walls and so does not change its wave function."

The atom clones were then compared at regular intervals using a technique called "quantum interference" to determine exactly when a significant change of the matter wave occurred. The height above the bottom of the light bowl was varied at the start of the experiment to control the atom's "position energy." Technion Prof. Yoav Sagi explained: "We were able to demonstrate that the minimum time for the matter wave to change depends on this energy uncertainty. The greater the uncertainty, the shorter the Mandelstam-Tamm time."

While these results aligned with the predictions of the two Russian researchers, another effect that was discovered did not. When the physicists increased the energy uncertainty "until it exceeded the average energy of the atom, then the minimum time did not decrease further - contrary to what the Mandelstam-Tamm limit would actually suggest." The new findings proved that there is a speed limit imposed by the atom's average energy.

The study was funded by the Reinhard Frank Foundation in collaboration with the German Technion Society, the German Research Foundation (DFG), the Helen Diller Quantum Center at the Technion, and the German Academic Exchange Service (DAAD).

10.CISA, FBI and NSA Publish Joint Advisory and Scanner for Log4j Vulnerabilities

by Ravie Lakshmanan
https://thehackernews.com/2021/12/cisa-fbi-and-nsa-publish-joint-advisory.html

Cybersecurity agencies from Australia, Canada, New Zealand, the U.S., and the U.K. on Wednesday released a joint advisory in response to widespread exploitation of multiple vulnerabilities in Apache's Log4j software library by nefarious adversaries.

"These vulnerabilities, especially Log4Shell, are severe," the intelligence agencies said in the new guidance. "Sophisticated cyber threat actors are actively scanning networks to potentially exploit Log4Shell, CVE-2021-45046, and CVE-2021-45105 in vulnerable systems. These vulnerabilities are likely to be exploited over an extended period."

An attacker can exploit Log4Shell (CVE-2021-44228) by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. CVE-2021-45046, on the other hand, allows for remote code execution in certain non-default configurations, while CVE-2021-45105 could be leveraged by a remote attacker to cause a denial-of-service (DoS) condition.

Since the vulnerabilities became public knowledge this month, unpatched servers have come under siege from ransomware groups to nation-state hackers, who have used the attack vector as a conduit to gain access to networks to deploy Cobalt Strike beacons, cryptominers, and botnet malware.

The U.S. Federal Bureau of Investigation's (FBI) assessment of the attacks has also raised the possibility that threat actors are incorporating the flaws into "existing cyber criminal schemes that are looking to adopt increasingly sophisticated obfuscation techniques." In light of the severity of the vulnerabilities and likely increased exploitation, organizations are being urged to identify, mitigate, and update affected assets as soon as possible.

To that end, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has also released a scanner utility to identify systems vulnerable to the Log4Shell vulnerability, mirroring a similar tool released by the CERT Coordination Center (CERT/CC).

However, Israeli cybersecurity firm Rezilion, in an assessment published this week, found that commercial scanning tools were ill-equipped to detect all formats of the Log4j library in an environment due to the fact that the instances are often deeply nested in other code, revealing the "blindspots" in such utilities and the limitations of static scanning.

"The biggest challenge lies in detecting Log4Shell within packaged software in production environments: Java files (such as Log4j) can be nested a few layers deep into other files — which means that

a shallow search for the file won't find it," Yotam Perkal, vulnerability research lead at Rezilion, said. "Furthermore, they may be packaged in many different formats which creates a real challenge in digging them inside other Java packages."

The public disclosure of Log4Shell has also led a number of technology suppliers to deploy patches for software that contain the flaw. The latest companies to issue updates are NVIDIA and HPE, joining a long list of vendors that have published security advisories detailing the products that are affected by the vulnerability.

The latest step taken by the governments arrives as the Apache Software Foundation (ASF) on Monday released updates for Apache HTTP Server to address two flaws — CVE-2021-44790 (CVSS score: 9.8) and CVE-2021-44224 (CVSS score: 8.2) — the former of which could be weaponized by a remote attacker to execute arbitrary code and take control of an affected system.

11.To keep our country safe, we need a national Cyber Academy

by Kirsten Gillibrand
https://www.washingtonpost.com/opinions/2021/12/23/keep-our-country-safe-we-need-national-cyber-academy-think-it-west-point-technology-defense/

Cybersecurity is undoubtedly one of the United States' most important lines of defense, but too many parts of the government don't have the reinforcements they need. In one of the most serious examples of danger, Russian hackers in 2019 penetrated SolarWinds software widely used by the U.S. government, and the hack went undetected for months. Networks ranging from the departments of Energy, Treasury and Justice to the National Institutes of Health were exposed to exploitation.

Unfortunately, the government faces a severe shortage of cyber personnel needed to protect ourselves from such adversaries. As of September, more than one-third of public-sector cybersecurity jobs — more than 38,000 — were unfilled. And the tech workforce we do have is quickly aging out: By our calculations, just 7 percent of federal employees in computer science, computer engineering and information technology positions are under 30.

We need to take bold, forward-looking action to build not only a new generation of cybersecurity and technology professionals, but also a new pipeline to cyber and tech careers in government. We need to establish a Cyber Academy.

Working with colleagues on the Senate Armed Services Committee, I recently secured provisions in the National Defense Authorization Act, the annual defense budget bill, that will jumpstart our work to do just that. They would create a roadmap for establishing, building and devising a curriculum for an institution that would staff up the federal cyber workforce and prepare the next generation of civil servants for the vital jobs of the 21st century.

The Cyber Academy we envision would be a state-of-the-art civilian counterpart to West Point, the Air Force Academy and other military academies — a government-funded university dedicated to training cyber and tech professionals for the civil service. It would make the U.S. government a vanguard in digital careers, while providing talented and civic-minded young people with a free, postsecondary technological education and a way to serve their country.

Cyber Academy students would earn degrees in fields such as artificial intelligence, software engineering, cybersecurity, robotics and data science. They then would be placed for a prearranged term in corresponding roles in various federal agencies, determined according to the government's digital and cyber needs and the students' preferences, and informed by our national security priorities.

These graduates would have important roles beyond defense. They could help us to protect the electric grid and food supply chain, oversee policies about cryptocurrency and develop regulations for complex machinery such as driverless cars and autonomous drones — and that's just scraping the surface.

The current tech workforce is neither large enough nor diverse enough to meet the nation's critical needs. There are currently more than 600,000 open computing jobs in the United States, but just 71,000 computer science students graduated into the workforce in 2020. And the government has to compete for them with private tech giants such as Google and Amazon. The Cyber Academy's service requirement would help address that uneven playing field and expedite the often slow-moving federal hiring process.

Recruiting for the Cyber Academy would also help us to diversify the field. The more perspectives, languages and skill sets we can bring into government, the more we can out-innovate and out-perform our competitors and counter looming technological threats from China and Russia. The Cyber Academy could make this education and these careers accessible to everyone, including nontraditional students and those from underserved communities.

Without an urgent strategic investment in strengthening our federal cyber workforce, we risk ceding global leadership to our competitors and falling behind on our ability to protect and advance our national interests. As it stands, we are not fully prepared to face the challenges and seize the opportunities ahead.

Experts in science, technology and national defense agree: Former Google chief executive Eric Schmidt said last year that establishing a type of cyber academy will help to address the "vast shortage of the talent" the United States needs to keep up "in a world shaped by strategic competition." Just last month, the Government Accountability Office published a report on the need for a "pipeline of digital staff," specifically noting that an academy could create a dedicated pool of talent with "proficiency in both digital skills as well [as] understanding the functions of government [required] to meet agencies' needs."

In the short term, the steady stream of tech talent from a Cyber Academy would enable the government to address its urgent personnel deficit. In the long term, it would build up a pool of digital and cyber experts, allowing the United States to gain substantial ground in technological innovation and cement our global leadership in the digital age.

12.Real-Time Error Correction for Quantum Computing

by Philip Ball
https://physics.aps.org/articles/v14/184

Random errors incurred during computation are one of the biggest obstacles to unleashing the full power of quantum computers. Researchers have now demonstrated a technique that allows errors to be detected and corrected in real time as the computation proceeds. It also allows error correction to be conducted several times on a single quantum bit (qubit) during the calculation[1]. Both features are needed to make the basic elements—the logical qubits—of a fully error-tolerant quantum computer that can be scaled up and used for applications beyond the specialized ones that these machines have tackled so far.

Error correction is straightforward on classical computers: by keeping several copies of each bit, a random error (such as a 1 flipping to a 0) can be identified and corrected using a simple majority rule. But that can't be done in quantum computers, since the computation relies on the qubits adopting quantum states that are neither 0 nor 1, and measuring them destroys those delicate states. So the states must remain unknown, and a fundamental principle forbids the copying of an unknown quantum state.

If qubit errors are not corrected, they will gradually accumulate and overwhelm the calculation with random noise, limiting the number of steps a quantum algorithm can reliably perform. The problem gets harder to manage as the number of qubits increases. That's why today's quantum computers have only a relatively small number of "noisy" qubits. The best of these quantum circuits may still outperform classical computers for certain types of calculations, but without quantum error correction (QEC), the power and scope of quantum computing remain limited.

Various QEC methods have been proposed in which several physical qubits are quantum mechanically entangled to make a single logical qubit that has some resistance to errors. But these schemes have typically allowed only one round of error correction for each logical qubit in a calculation. Another problem is that they have generally been retrospective—the final result is "post-corrected"—but not all errors can be corrected after-the-fact.

A team of researchers at Quantinuum (formerly Honeywell Quantum Solutions) in Broomfield, Colorado, has now implemented a method that overcomes some of these limitations. They use a QEC scheme first proposed in 1996 by Andrew Steane of the University of Oxford, UK[2]. Like most other QEC approaches, it involves additional so-called ancilla qubits, whose job is to signal errors in the "data qubits." In each of a series of operations, an ancilla qubit is entangled with a subset of data qubits, and then the

[1] C. Ryan-Anderson et al., "Realization of real-time fault-tolerant quantum error correction," Phys. Rev. X 11, 041058 (2021).

[2] A. M. Steane, "Error correcting codes in quantum theory," Phys. Rev. Lett. 77, 793 (1996).

ancilla qubit is measured. This process allows some information about the data qubits to be inferred without measuring them directly.

Although the basic idea has been around since the 1990s, putting it into practice with schemes for rapidly and repeatedly diagnosing and fixing the errors in a real quantum circuit with good-quality qubits posed a massive technological challenge. The algorithms and hardware developed by Ryan-Anderson and his colleagues now address these problems.

The researchers used qubits made from single ytterbium ions held in an electromagnetic trap. The system allows each ion to be moved into proximity with any other ion to enable the entanglement operations. The qubits are embodied in the quantum electronic states of the ions, which can be manipulated by laser beams. To read a qubit, the team hits the ion with a laser pulse and measures its fluorescence. Such trapped-ion quantum circuits are already being developed for commercial quantum computers. Ryan-Anderson and colleagues used ten of these physical-qubit ions to make a single error-tolerant logical qubit: seven of them were data qubits, and the other three were ancilla qubits.

The team showed that they could perform multiple rounds of error detection and correction on each data qubit in the circuit and that they could detect two distinct types of qubit errors. Previous efforts to achieve multiple error-correction rounds have only worked for one type. "Essentially, we have demonstrated for the first time all of the elements needed for a single [error-tolerant] logical qubit," says Ryan-Anderson.

"This is very high-caliber experimental work," says Steane. "It is one thing to deduce by analysis the effect of certain operations and measurements on qubits; it is quite another to achieve it in the lab," as the Honeywell team has now done. The work has "highlighted which parts of all the theoretical work on QEC and fault tolerance proved to be of practical use," says Steane.

"This is a significant advance," says Laird Egan, a quantum engineer at the Maryland-based company IonQ, which has previously implemented QEC methods for trapped-ion qubits. "What really distinguishes it is the multiple rounds of true fault-tolerant error correction"—something the IonQ team has not yet achieved.

QEC requires each logical qubit to be composed of multiple physical qubits, so the logical qubit incurs more potential sources of error than any of its component qubits. Ideally, the QEC can be fast enough that the logical qubit's error rate is lower than that of any physical qubit, but the Honeywell team's QEC, like all others developed so far, has not yet reached that level. So errors will still accumulate faster than they can be corrected. Reaching the so-called error-correction threshold, when QEC allows a logical qubit to outperform its physical qubits, "will be a big prize to whoever achieves it," Egan says. "I would not be surprised to see this threshold achieved in the next few years."

13.Quantum computing: Japan takes step toward light-based technology

by Akira Oikawa & Akihiro Ota
https://asia.nikkei.com/Business/Technology/Quantum-computing-Japan-takes-step-toward-light-based-technology

A Japanese team of scientists on Wednesday announced a key step in the development of a quantum computer using photons, or particles of light, that eliminates the need for an ultracold environment used to cool existing machines.

The team including Nippon Telegraph and Telephone, the University of Tokyo and Japan's Riken research institute has developed a high-performance source of "squeezed light" used to transmit information in optical quantum computing.

The goal is to develop a powerful quantum computer using this technology by 2030.

The public-private-academia effort marks a significant stride for Japan in an area that is expected to be vital for competition in a wide range of industries in the coming years. The government provided funding for the project as part of a 200 billion yen ($1.76 billion) initiative.

The field has largely been dominated by the U.S., thanks to tech giants such as Google and IBM, as well as by China, which is also at the forefront.

The research team sees the potential for vastly improved performance over competing technologies. "It's a paradigm shift," said project manager Akira Furusawa, professor at the University of Tokyo School of Engineering.

Optical computers can run at room temperature, without the expensive cooling equipment needed for other quantum computers that use superconductors.

NTT, which offers fiber-optic internet service in Japan and has continued to research optical technology, leveraged its experience and expertise in the field for this project.

Quantum computers can handle calculations that conventional systems cannot. Google announced in 2019 that it had achieved "quantum supremacy" by completing in just over three minutes a task that would take the best classical supercomputers 10,000 years. Companies and research institutions around the world have joined the race.

Google and IBM are working with superconducting quantum computers, which use materials that have zero electrical resistance at ultralow temperatures. In Japan, Riken and Fujitsu are taking this route as well.

The technology is advancing, with IBM announcing last month the development of a processor with 127 quantum bits, or qubits -- more than the 53-qubit system with which Google claimed quantum supremacy.

But there are certain hurdles, such as wiring, that make it difficult to improve the performance of superconducting systems, and other players are pursuing alternative possibilities.

Hitachi is working on a silicon-based quantum computer, seen as a promising avenue for large-scale systems in the future. U.S.-based IonQ uses trapped ions within a vacuum chamber.

Each of the available methods has advantages and disadvantages. The merits of optical systems include the potential for scalability and reduced power usage. China's University of Science and Technology said last year it had achieved quantum supremacy with a light-based computer.

Boston Consulting Group estimates that quantum computing will create $850 billion in annual value by 2040. While many challenges remain, such as dealing with errors caused by noise, the advances being made on multiple fronts could speed up the introduction of quantum technology into practical use.

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

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

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

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

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

- DISCOVERING NEW DRUGS

- CREATING BETTER BATTERIES
- PREDICTING THE WEATHER
- PICKING STOCKS
- PROCESSING LANGUAGE
- HELPING TO SOLVE THE TRAVELLING SALESMAN PROBLEM

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

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

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

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

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

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

- REDUCING CONGESTION
- PROTECTING SENSITIVE DATA

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

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

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

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

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

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

15.Researchers Disclose Unpatched Vulnerabilities in Microsoft Teams Software

by Ravie Lakshmanan
https://thehackernews.com/2021/12/researchers-disclose-unpatched.html

Microsoft said it won't be fixing or is pushing patches to a later date for three of the four security flaws uncovered in its Teams business communication platform earlier this March.

The disclosure comes from Berlin-based cybersecurity firm Positive Security, which found that the implementation of the link preview feature was susceptible to a number of issues that could "allow accessing internal Microsoft services, spoofing the link preview, and, for Android users, leaking their IP address, and DoS'ing their Teams app/channels."

Of the four vulnerabilities, Microsoft is said to have addressed only one that results in IP address leakage from Android devices, with the tech giant noting that a fix for the denial-of-service (DoS) flaw will be considered in a future version of the product. The issues were responsibly disclosed to the company on March 10, 2021.

Chief among the flaws is a server-side request forgery (SSRF) vulnerability in the endpoint "/urlp/v1/url/info" that could be exploited to glean information from Microsoft's local network. Also discovered is a spoofing bug wherein the preview link target can be altered to point to any malicious URL while keeping the main link, preview image and description intact, allowing attackers to hide malicious links and stage improved phishing attacks.

The DoS vulnerability, which affects the Android version of Teams, could cause the app to crash simply by sending a message with a specially crafted link preview containing an invalid target instead of a legitimate URL. The last of the issues concerns an IP address leak, which also affects the Android app. By intercepting messages that include a link preview to point the thumbnail URL to a non-Microsoft domain, Positive Security said it's possible to gain access to a user's IP address and user agent data.

"While the discovered vulnerabilities have a limited impact, it's surprising both that such simple attack vectors have seemingly not been tested for before, and that Microsoft does not have the willingness or resources to protect their users from them," Positive Security's co-founder Fabian Bräunlein said.

16.A-list candidate for fault-free quantum computing delivers surprise

by Rice University
https://phys.org/news/2021-12-a-list-candidate-fault-free-quantum.html

A Rice University-led study is forcing physicists to rethink superconductivity in uranium ditelluride, an A-list material in the worldwide race to create fault-tolerant quantum computers.

Uranium ditelluride crystals are believed to host a rare "spin-triplet" form of superconductivity, but puzzling experimental results published this week in Nature have upended the leading explanation of how the state of matter could arise in the material. Neutron-scattering experiments by physicists from Rice, Oak Ridge National Laboratory, the University of California, San Diego and the National High Magnetic Field Laboratory at Florida State University revealed telltale signs of antiferromagnetic spin fluctuations that were coupled to superconductivity in uranium ditelluride.

Spin-triplet superconductivity has not been observed in a solid-state material, but physicists have long suspected it arises from an ordered state that is ferromagnetic. The race to find spin-triplet materials has heated up in recent years due to their potential for hosting elusive quasiparticles called Majorana fermions that could be used to make error-free quantum computers.

"People have spent billions of dollars trying to search for them," Rice study co-author Pengcheng Dai said of Majorana fermions, hypothetical quasiparticles that could be used to make topological quantum bits free from the problematic decoherence that plagues qubits in today's quantum computers.

"The promise is that if you have a spin-triplet superconductor, it can potentially be used to make topological qubits," said Dai, a professor of physics and astronomy and member of the Rice Quantum Initiative. "You can't do that with spin-singlet superconductors. So, that's why people are extremely interested in this."

Superconductivity happens when electrons form pairs and move as one, like couples spinning across a dance floor. Electrons naturally loathe one another, but their tendency to avoid other electrons can be

overcome by their inherent desire for a low-energy existence. If pairing allows electrons to achieve a more sloth-like state than they could achieve on their own—something that's only possible at extremely cold temperatures—they can be coaxed into pairs.

The coaxing comes in the form of fluctuations in their physical environment. In normal superconductors, like lead, the fluctuations are vibrations in the atomic lattice of lead atoms inside the superconducting wire. Physicists have yet to identify the fluctuations that bring about unconventional superconductivity in materials like uranium ditelluride. But decades of study have found phase changes—watershed moments where electrons spontaneously rearrange themselves—at the critical points where pairing begins.

In the equations of quantum mechanics, these spontaneous ordered arrangements are represented by terms known as order parameters. The name spin triplet refers to the spontaneous breakdown of three symmetries in these ordered arrangements. For example, electrons spin constantly, like tiny bar magnets. One order parameter relates to their spin axis (think north pole), which points up or down. Ferromagnetic order is when all spins point the same direction, and antiferromagnetic order is when they alternate in an up-down, up-down arrangement. In the only confirmed spin-triplet, superfluid helium-3, the order parameter has no fewer than 18 components.

"All other superconductivity is spin singlet," said Dai, who's also a member of Rice's Center for Quantum Materials (RCQM). "In a spin singlet, you have one spin up and one spin down, and if you put a magnetic field on, it can easily destroy superconductivity."

That's because the magnetic field pushes spins to align in the same direction. The stronger the field, the stronger the push.

"The problem with uranium ditelluride is the field required to destroy superconductivity is 40 Tesla," Dai said. "That's huge. For 40 years, people thought the only possibility for that to occur is that when you put a field on, the spins are already aligned in one direction, meaning it's a ferromagnet."

In the study, Dai and Rice postdoctoral research associate Chunruo Duan, the study's lead author, worked with Florida State co-author Ryan Baumbach, whose lab grew the single crystal samples of uranium ditelluride used in the experiment, and UC San Diego co-author Brian Maple, whose lab tested and prepared the samples for neutron-scattering experiments at Oak Ridge's Spallation Neutron Source.

"What the neutron does is come in with a particular energy and momentum, and it can flip the Cooper pair spins from an up-up state to an up-down state," Dai said. "It tells you how the pairs are formed. From this neutron spin resonance, one can basically determine the electron pairing energy" and other telltale properties of the quantum mechanical wave function that describes the pair, he said.

Dai said there are two possible explanations for the result: either uranium ditelluride is not a spin-triplet superconductor, or spin-triplet superconductivity arises from antiferromagnetic spin fluctuations in a way that physicists haven't previously imagined. Dai said decades of experimental evidence points to the latter, but this appears to violate conventional wisdom about superconductivity.

So Dai teamed up with Rice colleague Qimiao Si, a theoretical physicist who specializes in emergent quantum phenomena like unconventional superconductivity.

Si, a study co-author, has spent much of the past five years showing a theory of multiorbital pairing he co-developed with former Ph.D. student Emilian Nica explains contradictory experimental findings in several kinds of unconventional superconductors, including heavy fermions, the class that includes uranium ditelluride.

In multiorbital pairing, electrons in some atomic shells are more likely to form pairs than others. Si recalled thinking that uranium had the potential to contribute paired electrons from any of seven orbitals with 14 possible states.

"Multiorbitals was the first thing that came to mind," he said. "It wouldn't be possible if you only had one band or one orbital, but orbitals bring a new dimension to possible unconventional superconductor pairings. They're like a palette of colors. The colors are the internal quantum numbers, and the f electrons in the uranium-based, heavy-fermion materials are naturally set up to have these colors. They lead to new possibilities that go beyond the 'periodic table of pairing states.' One of these new possibilities turns out to be spin-triplet pairing."

Si and Nica, who's now at Arizona State University, showed antiferromagnetic correlations could give rise to plausible, low-energy, spin-triplet pairing states.

"Spin-triplet pairing states are highly improbable in the vast majority of cases because pairs will form as spin-singlets in order to lower their energy," Si said. "In uranium ditelluride, spin-orbit coupling can change the energy landscape in a way that makes spin-triplet pairing states more competitive with their spin-singlet counterparts."

17.Quantum computing: Forget qubits, all the cool kids are talking about qutrits now

by Joel Khalili
https://www.techradar.com/news/quantum-computing-forget-qubits-all-the-cool-kids-are-talking-about-qutrits-now

Quantum computing company Rigetti has announced it is exploring experimental new hardware configurations that could improve the performance of its quantum processors.

As explained in a blog post, the firm has introduced a third energy state to its qubits, thus turning them into qutrits. According to Rigetti, doing so allows for significantly more information to be manipulated, while also decreasing readout errors by up to 60%.

"Accessing the third state in our processors is useful for researchers exploring the cutting edge of quantum computing, quantum physics and those interested in traditional qubit-based algorithms alike," the company explained.

Rigetti is currently offering access to qutrit operations via Quil-T, its pulse-level extension to the Quil instruction set architecture.

Behold, the qutrit

A quantum bit (or qubit) is the smallest unit of quantum information, an analogue to the binary bit of classical computing. However, unlike the traditional bit, a qubit can adopt a value of one, zero or anything in between by virtue of a phenomenon known as superposition.

"Qubits are the basic building block of a quantum processor, and are so named because they represent a continuum of complex superpositions of two basic quantum states," explains Alex Hill, Senior Quantum Systems Engineer at Rigetti.

"The power of qubits comes in part from their ability to encode significantly more information than a classical bit – an infinite set of states between 0 and 1."

Historically, researchers have attempted to achieve quantum advantage (the point at which quantum systems outstrip traditional supercomputers in a meaningful way) by focusing on increasing the number of qubits on a quantum processor. Simply put, the larger the number of qubits, the more powerful the quantum machine.

Just last month, for example, IBM unveiled a record-breaking 127-qubit processor, codenamed Eagle. And Rigetti itself now offers an 80-qubit processor (the Aspen-11), created by linking two separate 40-qubit processors together.

However, Rigetti contends that the addition of a third state to qubits, creating a three-level quantum system based on qutrits, represents another path to improving the performance of quantum machines.

"With carefully-chosen readout parameters, classification performance can be significantly better when choosing between |2> and |0>, rather than the default classification between |0> and |1>," the company explained.

In future, it might even be possible to push towards qubits with an even larger number of states, says Rigetti. However, because an ever-smaller amount of energy separates states beyond zero and one, noise and control issues become increasingly difficult to surmount.

18.Here's how cybersecurity threats will evolve in 2022

by Tech Desk
https://indianexpress.com/article/technology/crypto/heres-how-cyber-threats-will-evolve-in-2022-7683494/

An increase in scams related to cryptocurrency, more data breaches, and frequent identity thefts and frauds are some of the top cybersecurity predictions for 2022 from Palo Alto Network.

According to cyber security firm Palo Alto Networks, in 2021, the impact of ransomware attacks reached an unprecedented scale, posing a threat to thousands of businesses around the world and threatening their critical infrastructure. And this trend will continue to be observed in 2022 as well.

Here's a look at Palo Alto Network's top cybersecurity predictions for 2022.

Rise of scams fuelled by Bitcoin

Cryptocurrency, in particular Bitcoin, will fuel the rise and evolution of the ransomware industry, with larger attacks on important infrastructure, while calls for its regulation will gain traction. The company said in its report that due to its decentralized character, it will be difficult for regulators to track down the hackers.

Bitcoin is a decentralized currency, which means it is not regulated by any government or organisation. Most often, threat actors demand ransomware payments in cryptocurrency because this form of payment provides anonymity for the destination address associated with the ransom demand. Unlike bank accounts, no personally identifiable information is required to obtain a crypto wallet.

"Businesses must concentrate on enhancing their cybersecurity posture and determining their level of preparedness for an attack, as well as conducting exercises to identify any security weaknesses that must be fixed," the company said, adding that collaboration between cybersecurity providers, cloud providers, and telecommunications providers "will help disrupt successful attacks and impose real costs on attackers."

Countries' critical digital infrastructure in the crosshairs

Increased usage of smart devices, will create tonnes of digital data that will double up in 2022. It should be noted the more data we produce, the problematic it becomes in terms of storing the data securely.

According to Palo Alto Networks, organizations need to draw up a strategic approach that will provide complete visibility into the security infrastructure. The company recommends a Zero Trust architec-

ture combined with Artificial Intelligence (AI). A zero trust architecture (ZTA) is an cybersecurity solution designed to prevent data breaches and limit any internal data leakage.

Cyberattacks on essential infrastructure, with confidential and lucrative data, worldwide, are on rise. These attacks have revealed that the implementation of cybersecurity protocols is significantly slower than the rate of digitalization across countries.

With hackers aiming to dent the critical infrastructure, "we need to fastrack improved global policies and regulatory collaboration. Governments and businesses must encourage the creation of safeguards against complex threats, particularly those that target critical infrastructure through supply chain gaps," the company highlighted.

Phishing will continue to dominate

Phishing emails and scams could evolve by next year. Cybercriminals have now switched their focus from targeting corporate offices to attacking individuals.

To contend with this new reality, enterprises will have to evolve beyond their corporate networks, deploy remote work solutions and bring unified security policy management to remote employees. "Combining security, networking, and digital experience management, SASE solutions will be critical in bringing about both security and operational efficiency," the company said in a blog post.

Identity frauds will rise

With the rise of open-banking and hyper growth of Fintech, poor programming or security misconfigurations could provide cybercriminals with greater opportunities to carry out identity theft, fraud, and unauthorized data collection.

Palo Alto Networks suggests special focus to be elderly groups, who may be more susceptible to fraud as they are the new users of digital banking platforms.

"Mitigating tomorrow's threats will require a greater leadership commitment, collaboration, and effective communication to drive a mindset shift to view cybersecurity as a team sport between governments, enterprises, and individuals," the company added.

19.Top 7 common Cybersecurity Myths — Busted

by The Hacker News
https://thehackernews.com/2021/12/top-7-common-cybersecurity-myths-busted.html

Even with the growing awareness about cybersecurity, many myths about it are prevalent. These misconceptions can be a barrier to effective security.

The first step to ensure the security of your business is to separate the false information, myths, and rumors from the truth.

Here, we're busting some common cybersecurity myths. Read on to find out which of the following you thought were true.

Cybersecurity Myths vs. Truths

Myth #1 — Too much security diminishes productivity

There is a common idea that increased security makes it difficult for even employees to access what they need, not just hackers. Strict security policies such as regular monitoring and access control are believed to hinder productivity at work. However, doing away with security may have far-reaching consequences for your business. A successful attack like a DDoS attack or ransomware can bring your business to a standstill. Employees might not be able to access important files, networks, and information after an attack. The recovery takes days and sometimes even weeks.

Truth: Enhanced cybersecurity can boost productivity.

A modern cybersecurity approach uses security tools that have a built-in security feature that integrates seamlessly into your system. It also leverages advanced tech intelligence and analytics for real-time detection and mitigation of threats. This allows developers to concentrate on improving their productivity since they no longer need to worry about security issues.

Myth #2 — Cyberattacks are only caused by external threat actors

Insider threats are on the rise and are fast becoming a cause of concern for businesses. Insider threats can include employees, vendors, contractors, business partners, or an external intruder trying to impersonate an employee. A recent survey revealed that insider threats are responsible for 60% of data breaches.

In addition, you can never be fully aware of where these attacks can originate from, and traditional security solutions are largely ineffective when it comes to these threats. This makes them much harder to detect and contain than external threats.

Truth: Therefore, cyberattacks can very well start from someone you know.

Use a combination of behavioral analytics and privilege and access management to minimize insider threats. Additionally, conduct security awareness training sessions to educate employees about the dangers of insider threats and how to detect them.

Myth #3 — Cybercriminals only attack large businesses

Small and medium-sized businesses may often be under the false impression that their data isn't valuable to hackers. However, small and medium-sized businesses are one of the top targets for hackers.

A recent study revealed that hackers targeted small businesses nearly half of the time. But only 14% of these businesses were prepared to defend themselves in such a situation.

Truth: No business - no matter how large or small, is ever immune to hacking attempts and malicious attacks.

Hackers don't discriminate when it comes to their victims. So, don't let the size of your business, determine how valuable your data is or how secure your assets are.

Myth #4 — Anti-Virus or Anti-Malware Software is enough to secure my business

The anti-virus software is an essential part of your cybersecurity plan. However, it only secures one entry point into your system. Hackers have many ways to bypass anti-virus software and infiltrate networks with attacks such as targeted phishing attacks, and ransomware.

So, even with anti-malware software in place, hackers will have plenty of room to launch an attack.

Truth: Anti-virus software can only protect you from a unique set of recognized cyber threats, not from other emerging cyber threats.

As a business, you need to do much more to secure your data from hackers. Deploy an all-encompassing security solution like a Web Application Firewall that monitors threats continuously and provides end-to-end, 24*7 protection from cyber risks.

Myth #5 — Cybersecurity is too expensive

Even as malicious cyberattacks continue to make headlines and cost businesses millions, companies still wonder if cybersecurity investments are worth it. Data security is frequently overlooked and is only an afterthought for many enterprises. The average cost of a data breach in 2021 is $4.24 million, the highest in the last 17 years. And this figure does not include the damage that comes with the crippling reputational losses and customer losses from a breach.

Truth: The cost of a good cybersecurity solution is nothing compared to the cost of a successful attack.

Invest in a modern security solution like Indusface AppTrana, for example, that can protect you from the latest threats. Moreover, there are many precautionary measures that you can take with absolutely no additional cost to your business, such as strong passwords, multi-factor authentication, access management, and employee training.

Myth #6 — You don't require cybersecurity because you've never been attacked

If you've never experienced a cyberattack or data breach yourself, the chances are that you don't know just how much damage they can cause. You may also assume that your current security posture is strong enough to keep the bad actors away since you've never been attacked.

However, cyber threats and hacking tools are continuously evolving to become more and more sophisticated and undetectable each day. And any sensitive data is a potential target for a breach.

Truth: You could easily be the next target.

Develop a sound security strategy that helps you identify existing weaknesses and mitigate attack attempts before any significant damage is caused.

Myth #7 — You've achieved total cybersecurity

Cybersecurity is a continuous process that needs to be upgraded with the changes in the threat landscape. Therefore, never stop working on securing your IT assets. Your organization will always be susceptible to existing and emerging threats.

Truth: There is no such thing as total or perfect cybersecurity against cyberattacks.

Review your security policies periodically, conduct security audits, monitor your critical assets continuously, and invest in the upcoming updates in security measures.

Conclusion

Myths and negative ideas around cybersecurity pose a real threat to organizations that are exposed to various cyber threats each day. Misinformation can open even more opportunities for hackers to infiltrate your network. Stay informed on the latest security best practices to ensure the safety of your business and customers.

20.Quantum Communication With Itinerant Surface Acoustic Wave Phonons

by É. Dumur, K. J. Satzinger, G. A. Peairs, M.-H. Chou, A. Bienfait, H.-S. Chang, C. R. Conner, J. Grebel, R. G. Povey, Y. P. Zhong & A. N. Cleland
https://www.nature.com/articles/s41534-021-00511-1

Surface acoustic waves are commonly used in classical electronics applications, and their use in quantum systems is beginning to be explored, as evidenced by recent experiments using acoustic Fabry–Pérot resonators. Here we explore their use for quantum communication, where we demonstrate a single-phonon surface acoustic wave transmission line, which links two physically separated qubit nodes.

Each node comprises a microwave phonon transducer, an externally controlled superconducting variable coupler, and a superconducting qubit. Using this system, precisely shaped individual itinerant phonons are used to coherently transfer quantum information between the two physically distinct quantum nodes, enabling the high-fidelity node-to-node transfer of quantum states as well as the generation of a two-node Bell state. We further explore the dispersive interactions between an itinerant phonon emitted from one node and interacting with the superconducting qubit in the remote node. The observed interactions between the phonon and the remote qubit promise future quantum-optics-style experiments with itinerant phonons.

21.Cybersecurity Company Identifies Months-Long Attack On Us Federal Commission

by Jonathan Greig
https://www.zdnet.com/article/cybersecurity-company-identifies-months-long-attack-on-us-federal-commission/

The United States Commission on International Religious Freedom (USCIRF) has been hit with a cyberattack, according to cybersecurity firm Avast.

Avast did not identify the federal agency affected, but The Record was able to determine it was the USCIRF.

The Cybersecurity and Infrastructure Security Agency (CISA) declined to comment on the attack and said all requests for more information should go to USCIRF. USCIRF did not respond to requests for comment.

Created in 1998, USCIRF describes itself as a US federal government commission that monitors the right to freedom of religion or belief abroad.

"USCIRF uses international standards to monitor religious freedom violations globally, and makes policy recommendations to the President, the Secretary of State, and Congress," the organization said on its website.

In Avast's report, the company said attackers were able to compromise systems on USCIRF's network in a way that "enabled them to run code as the operating system and capture any network traffic traveling to and from the infected system."

The report notes that there is evidence that the attack was done in multiple stages and may have involved "some form of data gathering and exfiltration of network traffic."

"Further because this could have given total visibility of the network and complete control of an infected system, it is further reasonable speculation that this could be the first step in a multi-stage attack to penetrate this or other networks more deeply in a classic APT-type operation," Avast said.

"That said, we have no way to know for sure the size and scope of this attack beyond what we've seen. The lack of responsiveness is unprecedented and cause for concern. Other government and non-government agencies focused on international rights should use the IoCs we are providing to check their networks to see if they may be impacted by this attack as well."

Avast said the attack has been going on for months, yet USCIRF and CISA refused to engage with them when notified. They allegedly tried multiple channels over the course of months to help resolve the issue but were ignored after initial communications.

"The attempts to resolve this issue included repeated direct follow-up outreach attempts to the organization. We also used other standard channels for reporting security issues directly to affected organizations, and standard channels the United States Government has in place to receive reports like this," Avast explained.

"In these conversations and outreach, we have received no follow up, or information on whether the issues we reported have been resolved and no further information was shared with us. Because of the lack of discernible action or response, we are now releasing our findings to the community so they can be aware of this threat and take measures to protect their customers and the community."

An Avast spokesperson told ZDNet that after the report was published, they were contacted by CISA.

The company admitted that their analysis was based on two files they observed in the attack and noted that without more information from USCIRF, it was hard to know who the attackers were, what their motive is and the potential impact of the attack.

The Avast spokesperson said that with the ability to intercept and possibly exfiltrate all local network traffic from USCIRF, the backdoor "had the potential to give the attackers total visibility of the network including information exchanged with other agencies, or international governmental or non-governmental organizations, and complete control of the agencies' system."

"Fixing the issue, therefore, is essential, however since the agency didn't respond to us, we can't tell whether the issues we reported have been resolved," the spokesperson said.

"Taken all together, this attack could have given total visibility of the network and complete control of a system and thus could be used as the first step in a multi-stage attack to penetrate this, or other networks more deeply."

It has been about one year since the SolarWinds attack, where hackers for the Russian government spent months inside the systems of multiple US government agencies, including the Justice Department, Treasury Department, Department of Homeland Security, State Department and Department of Energy.

22.Phishing Remains Top Form Of Cyber-security Breach In 2021

by Stu Sjouwerman
https://blog.knowbe4.com/phishing-remains-top-form-of-cybersecurity-breach-in-2021?utm_content=191839588&utm_medium=social&utm_source=linkedin&hss_channel=lis-TEZp_Z6yIE

Over half of organizations say they've experienced a cybersecurity breach caused by phishing in the last 12 months, dwarfing the second-place breach cause (malware) by almost 30%.

The latest data from Dark Reading's annual Strategic Security Survey shows phishing continues to be an organization's biggest problem. With 53% of organizations citing phishing as being the cause of a security breach (up from 51% in 2020), organizations are keenly aware of the problem that exists when mixing users, social engineering, and phishing emails.

According to the survey:

- 58% say Users being socially engineered via phishing or other scams is the most significant endpoint security concern
- 48% of respondents say that if their organization experiences a major data breach in the next 12 months, the most likely cause will be a negligent end user.

So, users are definitely the weak link in the security chain in most organizations. And this requires some shoring up of security efforts around users, including Security Awareness Training to turn the user from a security liability to an asset who aids in protecting the organization.

According to the survey, of those organizations that experienced a cybersecurity breach in the last 12 months, 23% reported network disruptions and application unavailability, 17% say they experienced a major financial loss, and 15% reported fraud.

Phishing and the user have been proven to be an effective initial attack vector. And with the potential damage an attack can have, it's imperative to strengthen every part of your security stance – including the user.

23.New Performance Benchmark: Measuring A Quantum Computer's Power Just Got Faster And More Accurate

by Sandia National Laboratory
https://scitechdaily.com/new-performance-benchmark-measuring-a-quantum-computers-power-just-got-faster-and-more-accurate/

What does a quantum computer have in common with a top draft pick in sports? Both have attracted lots of attention from talent scouts. Quantum computers, experimental machines that can perform some tasks faster than supercomputers, are constantly evaluated, much like young athletes, for their potential to someday become game-changing technology.

Now, scientist-scouts have their first tool to rank a prospective technology's ability to run realistic tasks, revealing its true potential and limitations.

A new kind of benchmark test, designed at Sandia National Laboratories, predicts how likely it is that a quantum processor will run a specific program without errors.

The so-called mirror-circuit method, published today (December 20, 2021) in Nature Physics, is faster and more accurate than conventional tests, helping scientists develop the technologies that are most likely to lead to the world's first practical quantum computer, which could greatly accelerate research for medicine, chemistry, physics, agriculture, and national security.

Until now, scientists have been measuring performance on obstacle courses of random operations.

But according to the new research, conventional benchmark tests underestimate many quantum computing errors. This can lead to unrealistic expectations of how powerful or useful a quantum machine is. Mirror-circuits offer a more accurate testing method, according to the paper.

A mirror circuit is a computer routine that performs a set of calculations and then reverses it.

"It is standard practice in the quantum computing community to use only random, disordered programs to measure performance, and our results show that this is not a good thing to do," said computer scientist Timothy Proctor, a member of Sandia's Quantum Performance Laboratory who participated in the research.

The new testing method also saves time, which will help researchers evaluate increasingly sophisticated machines. Most benchmark tests check for errors by running the same set of instructions on a quantum machine and a conventional computer. If there are no errors, the results should match.

However, because quantum computers perform certain calculations much faster than conventional computers, researchers can spend a long time waiting for the regular computers to finish.

With a mirror circuit, however, the output should always be the same as the input or some intentional modification. So instead of waiting, scientists can immediately check the quantum computer's result.

The research was funded by the Department of Energy's Office of Science and Sandia's Laboratory Directed Research and Development program. Sandia is a leading member of the Quantum Systems Accelerator, a Department of Energy national quantum research center.

New method reveals flaws in conventional performance ratings

Proctor and his colleagues found that randomized tests miss or underestimate the compound effects of errors. When an error is compounded it grows worse as the program runs, like a wide receiver who runs the wrong route, straying farther and farther from where they are supposed to be as the play goes on.

By mimicking functional programs, Sandia found final results often had larger discrepancies than randomized tests showed.

"Our benchmarking experiments revealed that the performance of current quantum computers is much more variable on structured programs" than was previously known, Proctor said.

The mirror-circuit method also gives scientists greater insight into how to improve current quantum computers.

"By applying our method to current quantum computers, we were able to learn a lot about the errors that these particular devices suffer — because different types of errors affect different programs a different amount," Proctor said. "This is the first time these effects have been observed in many-qubit processors. Our method is the first tool for probing these error effects at scale."

24.NIST Post Quantum Crypto Timelines: Avoiding The Dangerous Misconception

by Alan Grau
https://technative.io/nist-post-quantum-crypto-timelines-avoiding-the-dangerous-misconception/

In response to the threat to RSA and ECC encryption algorithms imposed by Quantum Computers, the National Institute of Science and Technology (NIST) has been leading an effort to define replacement cryptographic algorithms

The goal is to create standards for new asymmetric encryption algorithms capable of withstanding attacks from Quantum Computers.

NIST started this process started in 2015 and has stated that fully published standards will be available in 2024.

The new Post Quantum Crypto algorithms will replace RSA and ECC for a wide variety of applications and use cases. Conversion to new algorithms is a major undertaking, impacting PKI systems, TLS and VPN protocols, crypto libraries, HSMs, TPMs and a host of other systems. Rolling out these new algorithms across the entire ecosystem and supply chain will take years. If companies don't already have a roadmap for migration to PQC, they need to start now.

NIST timeline misconception

With NIST standards expected in 2024, some assume that we must wait until 2024 to begin implementing post quantum crypto solutions. This is a misconception. NIST has stated that they plan to announce the algorithms to be standardized in December of 2021 or January of 2022. In just a few months, we will know what algorithms will be standardized. In fact, NIST has already announced XMSS and LMS as standards for hash-based signature algorithms.

By early 2022 companies can begin implementing the Post Quantum Crypto solutions based on standardised algorithms. Implementations of these algorithms are available, so companies don't have to wait until 2024 to begin migration from classical crypto solutions to the new Post Quantum Crypto (PQC) algorithms.

Although implementation details may change to some degree between now and 2024, we should begin using these algorithms as soon as they are announced. Software updates allow libraries to support modifications to the algorithms. Hardware implementations can also handle changes to algorithm parameters and details by taking advantage of HW-SW codesign principles.

Given the magnitude of the effort required for migration to post quantum crypto algorithms, this is very good news.

Migration to Post Quantum Crypto

Enterprises should begin developing a plan to migrate their systems to Post Quantum Crypto algorithms. This process begins with education. Many companies are even forming their own crypto centres of excellence with dedicated staff to lead this effort.

Next, companies need to create an inventory of crypto solutions. This means conducting a comprehensive audit of the company's cyber infrastructure and gathering a broad set of information including:

- What devices, systems, programs, and servers are using cryptography?
- What algorithms are used?
- What is the purpose of each implementation?
- What type of cryptography is used by each?
- Is this cryptography implemented in a software library? Or in hardware?

Once this information has been gathered, companies can begin working on a roadmap to migration systems. There are six hey steps that should be taken for the migration to Post Quantum Cryptography Algorithms, the first four of which can take place today. These include:

- Education of the quantum threat
- Inventory of internal cryptography implementations
- Inventory of partner and supplier cryptography solutions
- Develop a roadmap for migration to PQC
- Implementation of PQC (multi-phased project)
- Testing and integration

Moving towards quantum security

We are much closer to having standards for PQC than some people realise. This is critical as many of the systems being designed and developed today will still be in use after quantum computers are able to break RSA and ECC encryption.

Company can, and should, act now and begin planning to migrate their systems to Post Quantum Cryptography. If we can take any lessons from the decade of work rolling out existing encryption standards, the first must be that failure to take action is simply delaying the inevitable.

25.Are We Prepared For Quantum-Based Security?

by Stephanie Kanowitz
https://gcn.com/emerging-tech/2021/12/are-we-prepared-quantum-based-security/359956/

The federal government may be underestimating the effort required to prepare for the threats posed by quantum computing.

The good news is there is still time to reduce those threats, said Duncan Jones, head of cybersecurity at Cambridge Quantum Computing. "Quantum is a two-sided coin, and on the positive side, we have quantum technology emerging now that can better protect U.S. interests against sophisticated cyberattacks -- and we can use quantum today to generate stronger cryptographic keys, for example," he said.

Quantum computers differ from classical ones in that the latter use bits of data – zeros and ones – while the former uses quantum bits, or qubits, which can take a range of values. As a result, quantum computers can accelerate problem-solving, including breaking today's cryptographic codes, which are essentially mathematical operations.

"Imagine someone gave you an open padlock. You can go attach that to anything you wanted to and shut it. Then you've got a problem because you can't open the padlock unless someone gives you the key," Jones said. "That's the kind of problem that we rely on in cryptography…. The challenge that quantum brings is that those mathematical problems that we've settled on as our commonly used ones are actually quite solvable in a quantum computer in the future."

In fact, a survey by the company found that of 104 U.S. federal government respondents, 76% believe new technologies, such as quantum, will break standard encryption, and 57% expect it to happen in the next two years.

What's more, 74% of respondents said they worry that a quantum-enabled cyberattack will happen without warning. Quantum computers are not yet powerful enough to break encryption, but those are the computers in development at companies that are open about their progress. What's happening behind closed doors or in unfriendly nation-states is a concern, Jones said.

.
.
.

Additionally, quantum attacks could work retrospectively, he added. For instance, a hacker could access and store sensitive data today, saving until quantum computers are sophisticated enough to decrypt it.

Sixty-four percent of respondents said they don't think they are ready to defend against these types of attacks, but it is possible to do so, Jones said, by making cryptographic keys unpredictable. One way to do that is to move away from using the mathematical basis of today's encryption schemes and toward a new one that neither classical nor quantum machines can break. The National Institute of Standards and Technology is leading this effort with the Post Quantum Cryptography standardization process.

"The NIST process will help ensure that these algorithms become standardized in [Federal Information Processing Standards] publications and are ready for consumption by federal authorities," Jones said.

The catch is that about a third of survey respondents are not aware of this work by NIST, and 32.7% have taken no action to prepare for quantum-enabled attacks. Still, almost 90% said they expect they'll be ready to defend against them within two years.

"I worry this indicates a lack of understanding of the effort involved," Jones said. "They need to start addressing the threat as soon as possible. It's a big task and leaving it longer is just putting more federal data at risk."

The standardization process for quantum also must move faster, he said. Last month, NIST and the United Kingdom's National Physical Laboratory signed a statement of intent to collaborate on quantum technologies, but "at the moment the advice from the U.S. government -- and to some extent the U.K. government as well -- is to wait a minute…. I'm not convinced that's great advice," Jones said.

While standards are being hashed out, agencies can start identifying where and how they use cryptography to protect their highest-value assets and exploring new technologies to get quantum-resistant production use cases up and running.

Several agencies are studying quantum. The White House Office of Science and Technology Policy announced in late 2020 the launch of Quantum.gov, the official website of the National Quantum Coordination Office, and released the "Quantum Frontiers Report," listing areas for research. NASA has a Quantum Artificial Intelligence Laboratory. In August, the Energy Department issued a request for information asking for access to quantum systems after Congress asked the department "to develop a roadmap to provide researchers access to quantum systems so as to enhance the U.S. quantum research enterprise, stimulate the fledgling U.S. quantum computing industry, educate the future quantum computing workforce, and accelerate advancement of quantum computer capabilities."

Over the summer, Axiom Space, which is building a commercial successor to the International Space Station, used Cambridge Quantum's Quantum Origin to communicate with ISS. The solution is a key-generation platform based on verifiable quantum entropy, meaning it uses quantum mechanics to generate cryptographic keys seeded with verifiable quantum randomness from Quantinuum's H-Series quantum computers, powered by Honeywell.

"Quantum is going to have an unbelievable impact on the world. I don't think people quite grasp how large it is," Jones said.

26.Why we need to consider the ethical implications of quantum technologies

by Mauritz Kop
https://physicsworld.com/a/why-we-need-to-consider-the-ethical-implications-of-quantum-technologies/

Research into quantum technologies has advanced so much over the past decade that the underlying science is rapidly being translated into real-world applications – be it quantum computers, materials or communications systems. But before these innovations are widely rolled out, I believe we must do more to address their ethical, legal and social implications.

It's easy to think that science has nothing to do with ethics, which is about the creation of universal rules and standards for moral behaviour. But there are ethical questions throughout science, whether it's artificial intelligence, nanotechnology, biotech or nuclear power. In fact, what's known as "quantum ethics" is an emerging field within applied ethics, which focuses on moral behaviour in specific domains.

Each of those domains has its own distinct properties, cases and societal impact, in which ethics applies. For example, the Hippocratic Oath taken by doctors exemplifies the moral responsibility of medical professionals towards their patients in upholding ethical standards such as helping the ill and pre-

scribing only beneficial treatments. Similarly, quantum technology has its own specific ethical challenges and dilemmas.

Theories of ethics that are considered useful regarding the values and motives of human conduct can be converted into practical rules, principles and responsibilities. At one level, universal ethical standards will apply to quantum technologies and, when determining those standards, we can use our "normative" ethical theories. Key principles that emerge from these theories are fairness, benevolence, nonmaleficence (avoiding harm), autonomy and sustainability.

In addition, the unique and counterintuitive phenomena that underpin quantum physics – such as superposition, entanglement and tunnelling – will require a tailored approach. Take quantum machine learning. The probabilistic nature of quantum mechanics means that deploying quantum algorithms and quantum data leads to different outcomes in terms of fairness and transparency (obligations and constraints) than drawing on classical methods, which raises ethical questions. In designing applied quantum ethics, cross-disciplinary research must be conducted into the consequences of the distinct features of applied quantum technology.

To see why we urgently need to address the ethics of quantum technology, consider these questions. How can we create equal access to a socially responsible quantum internet in developing countries? How should we use intellectual property and open-source instruments in an ethical way to prevent certain groups or businesses from monopolizing quantum computation and simulation, while still fostering innovation and ensuring equitable outcomes regarding benefits of the technology?

How, moreover, do we prevent human suffering from nefarious use of cryptographic items in the financial and energy sectors? What are the ethical concerns surrounding manipulating biological processes on the subatomic level and how can we make sure quantum machine-learning processes remain fair, democratic and unbiased? And how should we proceed when the principles of open science and innovation conflict with the desire to keep new information – such as discoveries in quantum materials science and engineering – undisclosed?

Coherent pathways

One possible definition of quantum ethics could be: "Quantum ethics calls for humans to act virtuously, abiding by the standards of ethical practice and conduct set by the quantum community, and to make sure these actions have desirable consequences, with the latter being higher in rank in case it conflicts with the former." Here we employ the old, familiar ethics that apply to all transformative technologies and to information. Due to the unique characteristics of quantum technologies, we also develop a new subtype of context-specific practical ethics.

This proposed definition allows different industries or economic sectors in which quantum systems, products and services operate to have their own sector-specific ethical rules. In the case of quantum-driven tools in neuroscientific medical R&D, for example, "neuroethics" generates ethical considerations about professional responsibility, personal identity and informed consent. Thus, a multi-layered, interdisciplinary ethical framework for quantum technology is formed.

The next step is to embed the quantum-specific ethical framework into a more comprehensive concept, dubbed "quantum-ELSPI", which describes the ethical, legal, social and policy implications of quantum technology. Such an approach would help us to regulate quantum technologies, the benefits and risks of which must be equally distributed across all members of society and across developed and developing countries in equal measure. Regulating quantum technology, therefore, requires a multidisciplinary approach that unifies perspectives from the humanities, natural and social sciences into evidence-based technology governance strategies.

Quantum ethics should not, however, be seen as a trade-off to innovation. Instead, inclusive, values-based, sustainable development will help reduce and remove barriers for translating technology into real-world commercial products. We must therefore develop structured methods that provide a coherent ethical pathway in which physicists can develop their ideas. This methodology should be endorsed by as many interested parties as possible, beginning with the quantum community itself.

We need to build bridges of mutual understanding between disciplines – a move that will involve learning to speak each other's language. This is easier said than done but the physics community must learn to understand the importance of ethics, its role in physics education and the ethical questions facing society. Bringing stakeholders together in a conference to establish a practical code of quantum ethics would be a crucial first step.

27.2021 in review: Jian-Wei Pan leads China's quantum computing successes

by Matthew Sparkes
https://www.newscientist.com/article/mg25233652-000-2021-in-review-jian-wei-pan-leads-chinas-quantum-computing-successes/

GOVERNMENTS and companies around the world are racing to build a useful quantum computer, and the stakes are as high as the R&D budgets. Such a machine could crack encryption wide open, boost the power of artificial intelligence and help develop unique materials and drugs.

A big player in the field is China, which has a centralised and extremely well-funded government project hoovering up talent, all under the oversight of one man: Jian-Wei Pan.

The same words crop up repeatedly when you discuss Pan with those who know him: reserved, focused, driven and bright. He is often referred to as the "father of quantum".

He attended the University of Science and Technology of China (USTC) in 1987 and later the University of Vienna in Austria for his doctorate, ultimately returning to USTC to run one of the largest and most successful quantum research groups in the world. In Vienna, he worked under the prominent physicist Anton Zeilinger, who later said: "I can't imagine the emergence of quantum technology without Jian-Wei Pan."

Gregor Weihs at the University of Innsbruck, also in Austria, worked with Pan in Vienna and recalls his time there. "Initially he didn't have any experimental experience, but it was obvious that he understood quantum physics better than any of us, and had amazingly creative ideas," he says.

"He was certainly driven and motivated to build bigger things," says Thomas Jennewein at the University of Waterloo in Canada, who also worked with Pan in Vienna and helped him set up a new quantum research lab at USTC in 2002.

After returning to China, Pan had a meteoric rise. He was elected to the Chinese Academy of Sciences in 2011, its youngest ever member, and the World Academy of Sciences the following year. He became vice-president of USTC in 2014.

Pan's work has yielded huge results – it has been cited in nearly 50,000 other scientific papers – and has in turn led to a lot of government investment. A quantum laboratory that was opened at USTC in 2020 cost a reported $10 billion. Such backing has yielded big results of late.

Tech giants and research teams around the world have been in a race to outdo each other when it comes to quantum supremacy, the point at which a quantum computer can solve a problem that is impossible for classical computers. In July 2021, USTC announced it had surpassed Google's claimed quantum supremacy achievement by solving a problem three orders of magnitude harder than that performed by Google's Sycamore machine. In September, USTC bested its own benchmark by another three orders of magnitude.

USTC is making great strides in quantum communication too. It recently revealed that the world's largest metropolitan quantum network – which involves banks, universities and government buildings across the city of Hefei in China – has been running for nearly three years. In 2016, USTC put the first quantum satellite into orbit, demonstrating unhackable communications with ground stations on Earth.

Pan's influence in Chinese science is large and growing. He is the vice-chair of the Jiusan Society, a minor political party that serves as a kind of think tank on scientific and educational issues.

It remains to be seen which country or company will be first to develop a practical quantum computer, but Pan and USTC seem likely to remain at the centre of this field for the near future.

28.How Quantum Encryption Can Improve Your Company's Data Security

by tidewateradmin
https://www.tidewaternews.com/uncategorized/how-quantum-encryption-can-improve-your-companys-data-security/

Data security is a hot topic in the world of business. Businesses are constantly looking for new ways to protect their data from hackers and other online threats. One type of encryption that has been gaining traction lately is quantum encryption, which uses entangled particles to transmit messages securely. This blog post will explore how quantum translation can improve your company's data security. So you can operate comfortably, knowing your information is safe.

First, let's take a step back and talk about quantum data encryption itself. Encryption is the process of converting information into a code that makes it unreadable to those without the key. Suppose you use an encrypted messaging app like Signal or Wickr Me. In that case, your messages are protected with cryptography, and only your contacts can read them. Otherwise, everyone on the internet could see your private information when two particles remain in communication if they wanted. It uses entangled particles as this "key" to lock up your data. To give you a little background, entanglement is connected even when separated by large distances. This happens because, at their core, they're actually one particle instead of two separate ones, no matter how far apart they may be from each other.

Once the data is encoded with quantum keys, it can be sent over any type of network or communication channel, including the internet. Quantum encryption is therefore perfect for companies that need to send sensitive information over an insecure network. Below are additional ways in which quantum inscribed can improve your company's data security:

Increased Security Against Hackers

As mentioned earlier, quantum conversion uses impossible particles to hack into. Even if a hacker was able to intercept your data, they would not be able to read it without the key. This makes quantum translation a very strong form of conversion and ideal for businesses that need extra security.

Increased Privacy

Along with increased security, quantum encryption also provides greater privacy for your data. Unlike traditional forms of encryption that use a single key, quantum conversion uses multiple randomly generated keys. This means that even if someone manages to get their hands on one of your keys, they won't be able to decrypt your data without the others. It's essentially impossible for anyone to hack into your data if it's encrypted with quantum keys.

Increased Compatibility

One of the best things about quantum conversion is that it's compatible with almost any type of device or network. This means you can use it to encrypt data regardless of the type of communication channel being used. It will work flawlessly whether you're using a cell phone, computer, or even a satellite.

Increased Efficiency

Quantum encryption is also more efficient than traditional conversion methods. This is because it doesn't require a lot of computational power to decode the data. This will make it suitable for use on

devices like smartphones and tablets. Also means that employees can use this to protect data wherever they are without slowing down their devices.

Faster Communication

Quantum conversion can actually speed up your communication process by allowing you to send messages without waiting for the keys to be generated. This is because quantum keys are already generated ahead of time. All you have to do is download them onto your device before sending information. With traditional coded methods, a key must be generated for each message sent. A secure connection must also be established between two parties before data transfer can begin.

Lighter Data

While this might not seem like a big deal, the fact that quantum-encrypted messages are lighter than traditional ones means it takes less time for them to get from point A to point B. This is especially important when considering how much sensitive information gets sent across the internet each day. Securing these messages with quantum conversion can save countless hours. This will also significantly reduce the costs associated with processing and storing data.

Standardized Networks

Finally, it will play an important role in ensuring all future networks around the world use standardized security methods and protocols. It's similar to how we all need electrical wiring in our homes and buildings for everything from appliances to lighting to work properly. We don't want wires that are incompatible with each other, right? It's the same thing with quantum translation. We want it to be the standard that ensures that all Internet communications are equally secure and private."

In conclusion, quantum conversion is a powerful form of data security that is quickly becoming the standard for businesses around the world. It provides increased security against hackers, greater privacy, and compatibility with almost any device or network. Additionally, quantum translation is more efficient than traditional methods, making it perfect for smartphones and tablets. Finally, it will play an important role in ensuring all future networks are standardized and secure.

29.How the Netherlands is forging ahead in quantum technologies

by Martijn Boerkam
https://physicsworld.com/a/how-the-netherlands-is-forging-ahead-in-quantum-technologies/

Freeke Heijman from Quantum Delta NL tells Martijn Boerkamp about the opportunities and challenges of quantum technologies

How did you get into quantum tech?

I graduated from the Technical University of Delft's Policy Analysis and Systems Engineering department in 1999 and after a two-year stint at KPN Research as a consultant, I joined the Ministry of Economic Affairs as an adviser in 2002. In 2013 – as head of strategy at the ministry – I visited the University of Technology in Delft to hear about their plans to start a quantum institute. Three years later the Netherlands held the presidency of the European Union and we helped to launch the €1bn Quantum Flagship programme. This led to interest from several Dutch research centres and companies, and to combine all this into a coherent national agenda I founded Quantum Delta NL last year together with Ronald Hanson and Jesse Robbers.

What is the role of Quantum Delta NL?

We are the Dutch umbrella organization that connects the five main quantum research hubs: Delft, Amsterdam, Leiden, Eindhoven and Twente. We bridge the gap between fundamental research and business, especially for start-ups that are taking quantum technology out of the lab and into people's lives. With the Netherlands being such a small country, it is easier for these institutes to collaborate and this type of collaboration is unique – we don't see it anywhere else. That's why we think the Netherlands can have a world-leading role in quantum technology over the next decade.

And what do you focus on?

My role is to foster the best ecosystem for quantum technology development. By removing barriers between institutions and procedures, and by focusing on talent and entrepreneurship, we want to establish an open culture where innovation is possible. We also want to go beyond quantum technology being a field only for physicists. To develop quantum products and services for society, other disciplines will be important such as computer science, design, business and law.

We want to go beyond quantum technology being a field only for physicists

Quantum Delta NL recently received €615m from the Dutch government. How will that be spent?

We support research and development in three main topics: quantum computing, quantum networks and quantum sensing. The next step is to give start-ups a better and faster way to market by building new cleanroom facilities so they can develop their technology as well as providing early-stage investment and a tailored acceleration programme dubbed Lightspeed. Additionally, we put extra effort into educating and attracting people as well as the social impact of quantum technology. A dedicated campus for this "quantum ecosystem" – called the House of Quantum – will be operational from 2024.

What is the Netherlands doing in quantum networks?

Last July saw the live demonstration of a quantum-encrypted video being transferred across a quantum connection between Delft and The Hague. Late November we went live with an advanced quantum internet through our Quantum Network Explorer (QNE). QNE is the "software stack" to run such a network. Currently it runs on an emulated quantum network but this will be upgraded to actual quantum hardware soon. We use these demonstrations to show the technology's capability to potential end-users and technology suppliers and give them a chance to participate.

What are the main challenges for Quantum Delta NL?

The main challenges are to scale up the ecosystem and engage with European industry. The key to these challenges is attracting and training the right talent. Even Quantum Delta NL has not reached the intended capacity yet, let alone attracting people into all the various programmes and start-up companies.

How does the Netherlands compare to the rest of the world?

The Netherlands is third in the world concerning quantum-research output and citations. Because we are nationally well organized, we are also frontrunners in developing the entrepreneurial ecosystem. However, European countries often lack the availability of venture capitalist funding or the big tech companies – both of which we see in the US, for example – that are willing to take the long-term risks. Fortunately, we see European industry engaging and EU governments investing. We also see some of the bigger companies, like Microsoft and Intel, collaborating with our research centres. On that level we are an important global player.

How do you see the interplay between competition and collaboration?

There will always be competition, but we mostly seek to collaborate. The development of quantum technology does not stop at the border – it requires effort on a global scale. On a European level we try to create a European ecosystem for quantum development. We are expanding through participation in several European programmes that have emerged from the quantum flagship programme. As an example, we work with several French institutions on topics such as spin-qubits and we also exchange talent with a job-board for quantum-related jobs in both countries.

Is there a danger that quantum technologies become a "bubble"?

There is a risk of overpromise, and we have a collective responsibility to manage this. Any mismatch between expectations and realization means part of the interest can collapse. We avoid that by tailoring our acceleration programme for start-ups and by only getting the right type of investors on board. But a little bit of hype is not necessarily bad as it will help to excite young talent to go into quantum technologies. As there is a solid scientific foundation underpinning the potential of quantum technology, the question is not if it will happen but when.

30.Rigetti Computing Announces Next-Generation 40Q and 80Q Quantum Systems

by Rigetti Computing
https://www.globenewswire.com/news-release/2021/12/15/2352647/0/en/Rigetti-Computing-Announces-Next-Generation-40Q-and-80Q-Quantum-Systems.html?utm_source=ActiveCampaign&utm_medium=email&utm_content=Rigetti+December+2021+Newsletter&utm_campaign=Rigetti+December+2021+Newsletter

Rigetti Computing, a pioneer in hybrid quantum-classical computing, today introduced its next-generation "Aspen-M" 80-qubit quantum computer into private beta. Aspen-M is the world's first commercial multi-chip quantum processor, solving a critical scaling challenge in the race toward fault-tolerant quantum computing. The Aspen-M processor leverages Rigetti's proprietary multi-chip technology and is assembled from two 40-qubit chips.

In addition, Rigetti announced it is collaborating with Deloitte, a multinational professional services company, and Strangeworks, a leading managed quantum service provider, to explore quantum applications in material simulation, optimization, and machine learning using Rigetti's new scalable processors.

Separately, a new Aspen system based on a single-chip 40-qubit processor will be released today for general availability on Rigetti Quantum Cloud Services, the Strangeworks Ecosystem, and Amazon Braket.

These latest Rigetti Aspen superconducting processors incorporate improvements in scale, speed, and fidelity—three metrics critical to unlocking broad commercial value. In addition to more than doubling the processor size over its previous generation, the systems powered by these processors deliver a 2.5x speedup in quantum processing times and reduce readout errors by up to 50 percent, drastically improving the reliability of quantum program results.

"With these systems, we've reached a critical milestone in the emerging quantum advantage era," said Chad Rigetti, founder and CEO of Rigetti Computing. "Our machines are now at a scale and speed where they can process the real-world data sets that underpin high-impact applications. We believe these systems give researchers and enterprises the best platform to pursue quantum advantage on real problems."

In one example using publicly available benchmark data from the New York Stock Exchange, the company performed a machine learning classification task that predicted whether the stock market would close higher or lower the following day. Results on both the 40Q and 80Q systems demonstrated quantum processing capabilities competitive with industry standard classical machine learning models. This example is an early demonstration of Rigetti's scale advantage, and it sets the stage for address-

ing problems of even greater computational complexity that remain inaccessible to existing classical computers.

In another early benchmark, the company targeted an optimization problem with 65 variables that was able to run on the Aspen-M system in under 5 minutes. Quantum algorithms of this scale are too large to simulate with classical computers, making Rigetti QCS what we believe to be the most broadly accessible platform for large-scale quantum algorithm development. This type of variational algorithm can be applied to a range of industry use cases including supply chain, logistics, and network optimization.

"As quantum computing continues to advance, organizations should explore the potential of quantum technologies to understand how they can advance their business models in the future," said Scott Buchholz, quantum computing leader, government and public services chief technology officer, and managing director, Deloitte Consulting LLP. "At Deloitte, we are collaborating with diverse technology providers and our clients to apply our combination of business and technology experience to define, design and engineer a tech-forward future. As part of this joint effort, we are looking forward to exploring Rigetti's new architecture jointly with Strangeworks to help clients define the right set of questions that will advance their stories."

"The scalability and speed of Rigetti's new processors is impressive and opens the door to new possibilities for quantum application developers and researchers," said William Hurley, founder and CEO of Strangeworks. "This kind of computing power enables enterprise-sized companies, like Deloitte, to apply quantum computing to problems of real importance. We're excited to work together with Deloitte and Rigetti to usher in a new era for quantum application development."

Rigetti expects the Aspen-M system to be publicly available in Q1 2022.

31.Quantum computing use cases are getting real—what you need to know

by Matteo Biondi, Anna Heid, Nicolaus Henke, Niko Mohr, Lorenzo Pautasso, Ivan Ostojic, Linde Wester, and Rodney Semmel
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know

Accelerating advances in quantum computing are serving as powerful reminders that the technology is rapidly advancing toward commercial viability. In just the past few months, for example, a research center in Japan announced a breakthrough in entangling qubits (the basic unit of information in quantum, akin to bits in conventional computers) that could improve error correction in quantum systems and potentially make large-scale quantum computers possible. And one company in Australia has developed software that has shown in experiments to improve the performance of any quantum-computing hardware.

As breakthroughs accelerate, investment dollars are pouring in, and quantum-computing start-ups are proliferating. Major technology companies continue to develop their quantum capabilities as well: companies such as Alibaba, Amazon, IBM, Google, and Microsoft have already launched commercial quantum-computing cloud services.

Of course, all this activity does not necessarily translate into commercial results. While quantum computing promises to help businesses solve problems that are beyond the reach and speed of conventional high-performance computers, use cases are largely experimental and hypothetical at this early stage. Indeed, experts are still debating the most foundational topics for the field (for more on these open questions, see sidebar, "Debates in quantum computing").

Still, the activity suggests that chief information officers and other leaders who have been keeping an eye out for quantum-computing news can no longer be mere bystanders. Leaders should start to formulate their quantum-computing strategies, especially in industries, such as pharmaceuticals, that may reap the early benefits of commercial quantum computing. Change may come as early as 2030, as several companies predict they will launch usable quantum systems by that time.

To help leaders start planning, we conducted extensive research and interviewed 47 experts around the globe about quantum hardware, software, and applications; the emerging quantum-computing ecosystem; possible business use cases; and the most important drivers of the quantum-computing market. In the report Quantum computing: An emerging ecosystem and industry use cases, we discuss the evolution of the quantum-computing industry and dive into the technology's possible commercial uses in pharmaceuticals, chemicals, automotive, and finance—fields that may derive significant value from quantum computing in the near term. We then outline a path forward and how industry decision makers can start their efforts in quantum computing.

32.Why China's Advancements in Quantum Technology Worry Others

by Ralph Jennings
https://www.voanews.com/a/why-china-s-advancements-in-quantum-technology-worry-others-/6355337.html

China's advances in quantum computing will give a new advantage to its armed forces, already the world's third strongest, analysts say.

Quantum refers to a type of computing that lets high-powered machines make calculations that are too complex for ordinary devices.

The concept discovered by American physicist Richard Feynman in 1980 has two key military uses, the think tank International Institute for Strategic Studies said in a 2019 paper. It can decrypt encoded messages and send cryptographic keys that intercept otherwise secure communication chains, the study says.

"I think the challenge is basically in the dual civilian-military strategy of China where the government will enlist the private sector into its military modernization program," said Alexander Vuving, professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies, in Hawaii. "Also, the government of China spends a lot of money in research and development."

China's name surfaced last month when IT consulting firm Booz Allen Hamilton said that within a decade Chinese "threat groups will likely collect data that enables quantum simulators to discover new economically valuable materials, pharmaceuticals, and chemicals."

China on the move

It's unclear how far Chinese researchers have advanced quantum computing, but the Pentagon's 2021 report to Congress on China says the Asian superpower "continues its pursuit of leadership in key technologies with significant military potential."

China's 14th Five-Year Plan, an economic blueprint, prioritizes quantum technology among other new fields, the report to Congress adds, and it intends to install satellite-enabled, global "quantum-encrypted communications capability" by 2030.

Quantum could help detect submarines and stealth aircraft among other "military vehicles," said Heather West, a senior research analyst with market research firm IDC in the U.S. state of Massachusetts. Quantum computing can break "classical algorithms" to check on another country's military, she told VOA.

The University of Science and Technology of China in Hefei last year made the first "definitive demonstration" of exploiting quantum mechanics for computations that would be "prohibitively slow on classical computers," the science journal Nature reported. Google and NASA had claimed "quantum supremacy" in 2019.

The state-run China Daily news website said in September the country had "achieved a series of breakthroughs in quantum technology including the world's first quantum satellite, a 2,000-km quantum communication line between Beijing and Shanghai, and the world's first optical quantum computing machine prototype." China Daily did not mention military use.

China has alarmed other countries in the past by merging civilian and military infrastructure, part of a Military-Civil Fusion Development Strategy that makes it hard for the outside world to judge when academic research will become an asset of the People's Liberation Army.

Although quantum computing worldwide remains at a "nascent stage," multiple countries are in a race to develop it, Vuving said. He points to the United States, India, Japan and Germany, in addition to China. Any frontrunners are unlikely to last long, he said, as rivals would quickly copy their breakthroughs.

Multiple countries at risk?

The Booz Allen Hamilton report says many organization leaders and chief information security officers "lack insight into the practical importance of quantum computing and how to manage related risks."

"They don't know how and when the technology might become useful — and how it might shape the behavior of threat actors such as China, a persistent cyber adversary of government and commercial organizations globally and a major developer of quantum-computing technology," the report says.

The People's Liberation Army maintains the world's third-strongest armed forces after the United States and Russia, according to the GlobalFirePower.com database. Japan, Taiwan and other Southeast Asian countries fret particularly over the expansion of the PLA Navy in disputed tracts of sea. Washington has stepped up military movement in the same seas since 2019 to monitor China's activities.

"Taiwan, the United States or the European Union are all likely targets for China to launch quantum computing attacks as long as countries do not have robust quantum cryptography to defend," said Chen Yi-fan, assistant professor of diplomacy and international relations at Tamkang University in Taiwan.

China is already suspected of using cyberattacks against Taiwan, a self-ruled island that Beijing says is part of its territory.

In the military realm outside China, quantum computing forms part of the AUKUS military technology sharing deal among Australia, the U.K. and the U.S. announced in September over Beijing's objections.

In August 2020, the White House, National Science Foundation and Department of Energy announced it would award $625 million over five years for quantum R&D, the National Defense Industrial Association says.

"We're seeing a lot of research and development going into the Department of Defense in the U.S.," West said. "I don't think they would be pouring the money into it if they didn't think there was that potential."

Researchers in Singapore, a well-off city-state, and Taiwan, a world tech hub, are exploring quantum technology as well.

Smaller countries couldn't compete with China's quantum computing resources, said Carl Thayer, emeritus professor of politics at the University of New South Wales in Australia. They would need engineers, technicians and money, he said.

"That's for the big boys, for the people with money, sophistication, knowledge. Other countries could toy around, but they wouldn't have the ability to go very far with it, I think," Thayer said.

33.US warns Log4j flaw puts hundreds of millions of devices at risk

by Liam Tung
https://www.zdnet.com/article/log4j-flaw-puts-hundreds-of-millions-of-devices-at-risk-says-us-cyber-security-agency/

Top US government cybersecurity officials fear advanced hackers will have a field day with the Log4j vulnerability that's likely present in hundreds of millions of devices.

Security experts are already seeing widespread scanning for the Log4j vulnerability (also dubbed 'Log4Shell') on internet-connected devices running vulnerable versions of Log4j version 2, which have been under attack since December 1, although the bug became common knowledge on December 9.

So far, Microsoft has seen attackers compromise machines to install coin miners, the Cobalt Strike pen-testing framework to enable credential theft and lateral movement, and exfiltration of data from compromised systems.

These attacks appear to be opportunistic cyber-criminal activity thanks to its ease of exploitation, but top officials at the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) fear "sophisticated actors" will also pounce on the bug soon.

"This vulnerability is one of the most serious that I've seen in my entire career, if not the most serious," Jen Easterly, director of CISA said in a call shared with CNN. Easterly has spent 20 years in various federal cybersecurity roles.

"We expect the vulnerability to be widely exploited by sophisticated actors and we have limited time to take necessary steps in order to reduce the likelihood of damage," she said. The call, with US critical infrastructure owners and operators, was first reported by CyberScoop.

Jay Gazlay of CISA's vulnerability management office warned that hundreds of millions of devices are likely to be affected.

Log4J is a popular Java library for logging error messages in applications. It's vulnerable to a critical flaw, tracked as CVE-2021-44228, that lets any remote attacker take control of another device on the internet, if it's running Log4J versions 2.0 to 2.14.1.

The remotely exploitable flaw is present in hundreds of major enterprise products, from the likes of Oracle, Cisco, RedHat, IBM, VMware and Splunk, and cloud features from Amazon Web Services and Microsoft Azure, as well as security appliances and developer tools. Google Cloud is investigating the impact of the Log4j bug on its products and services, and is working with VMware to deploy fixes to the Google Cloud VMware Engine. Google has updated WAF rules to defend against Log4j attacks.

The Apache Software Foundation has released version 2.15.0 to address the flaw, but product vendors still need to apply the fix in their products and then end-user customers need to update their devices once their vendor's fix becomes available.

The flaw highlights known risks arising from software supply chains when a key piece of software is used within multiple products across multiple vendors and deployed by their customers around the world.

t's not a simple fix to address all vulnerable devices. As Sans Internet Storm Center notes: "There is no generic 'log4j2' patch to patch everything. In some cases, vendors including Log4j, need to patch their software to include the new version."

Rapid7 had a similar warning: "Organizations should be prepared for a continual stream of downstream advisories from third-party software producers who include Log4j among their dependencies."

Rapid7 itself has been investigating its products' exposure to the Log4j bug and has deployed server-side fixes for several affected products.

Historically slow uptake of new security patches means attackers will likely have months if not years to find and exploit vulnerable devices, security experts warned this week.

The Log4j bug is internet-wide, prompting advisories from Australia, New Zealand, Canada, the UK, Sweden, Germany, Singapore, and elsewhere. Canada's Revenue Agency took some services offline on Friday after learning of the flaw, according to CBC.

34.Female-founded Indian Startup Getting Ready For Quantum Advantage

by James Dargan
https://thequantuminsider.com/2021/12/13/female-founded-indian-startup-getting-ready-for-quantum-advantage/

National Quantum Mission

With a huge population and an unlimited workforce that is educated and motivated, India is on the up as far as the future goes.

This is also the case in Deep Tech, where we can already witness several initiatives in this sector. This summer, for instance, the Indian government partnered with Intel India to launch an initiative to advance deep-tech-based research in the country.

In quantum computing (QC) too, actions like 2020's national quantum mission—which is being administered by the Ministry of Science and Technology—saw the country invest $1.12 billion over five years in the space.

The commercial scene has also seen growth with some really exciting players changing the face of the industry with BosonQ Psi, QpiAI and QuNu Labs three of a growing number. For more information about those and others in quantum from the subcontinent and other countries of APAC, please sign up to The Quantum Insider's very own data platform for better insight on this.

But back to India!

Another startup to add to the list, and a female-founded one at that, is Qkrishi. Set up this year and based in New Delhi, the nation's capital, Qkrishi's founders are Monika Aggarwal and Prabha Narayan. The two women established the startup to develop quantum models, algorithms and kernels for applications in automotive, finance, agriculture, seismology, signal processing, and other areas. Following in the footsteps of startups like ODE, founded by Keeper L. Sharkey, and Quantopticon, whose founders are Mirella Koleva and Gaby Slavcheva, the fact that they—along with Qkrishi—were started by women is a cool thing, but it doesn't define them.

Qkrishi

Qkrishi wants people to get ready for the quantum era. With a focus on building quantum technology with a combination of research and skilling, the team is working on an algorithm that will lead to Quantum Advantage.

It is doing this by building quantum-powered workflows to totally reshape how enterprises operate in sectors like automotive, finance, machine learning (ML), chemistry etc, and is working hard with customers to produce quantum teams that are effective through use cases that employ real and relevant data for the specific verticals.

> AT QKRISHI WE ARE ON A JOURNEY TO COMPLETELY CHANGE WHOLE INDUSTRIES AND BUSINESS MODELS
>
> —QKRISHI

As one of two Co-Founders and Directors at Qkrishi, Monika Aggarwal is also a Professor at the Indian Institute of Technology Delhi. An expert in quantum computing, signal processing, communications, and underwater technology, she obtained a Ph.D. in Electrical Engineering from the Indian Institute of Technology, Delhi.

An organization builder with vast experience in the automotive sector who founded a charity organization across two continents, Prabha Narayan has past experience as a Programmer Analyst for Daimler Chrysler on Assembly Plants Applications. She received a Bachelor of Engineering in Computer Science from SRM University, Chennai, Tamil Nadu.

35.Fast-Forwarding Quantum Evolution: Physical Features Boost the Efficiency of Quantum Simulations

by Los Alamos National Laboratory
https://scitechdaily.com/fast-forwarding-quantum-evolution-physical-features-boost-the-efficiency-of-quantum-simulations/

Two recent papers settle long-standing questions about algorithms on future quantum computers.

Recent theoretical breakthroughs have settled two long-standing questions about the viability of simulating quantum systems on future quantum computers, overcoming challenges from complexity analyses to enable more advanced algorithms. Featured in two publications, the work by a quantum team at Los Alamos National Laboratory shows that physical properties of quantum systems allow for faster simulation techniques.

"Algorithms based on this work will be needed for the first full-scale demonstration of quantum simulations on quantum computers," said Rolando Somma, a quantum theorist at Los Alamos and coauthor on the two papers.

Low-energy quantum states key to faster quantum simulation

The paper "Hamiltonian simulation in the low-energy subspace" demonstrates that the complexity of a quantum simulation algorithm depends on the relevant energy scale and not the full range of energies of the system, as previously thought. In fact, some quantum systems can have states of unbounded energies, hence simulations would prove intractable even on large quantum computers.

This new research found that, if a quantum system explores the low-energy states only, it could be simulated with low complexity on a quantum computer without errors crashing the simulation.

"Our work provides a path to a systematic study of quantum simulations at low energies, which will be required to push quantum simulations closer to reality," said Burak Sahinoglu, a theoretical physicist at Los Alamos and lead author on the paper, published in the journal Quantum Information, a Nature partner journal.

"We show that at every step of the algorithm, you never escape to the very large energies," said Somma. "There's a way of writing your quantum algorithm so that after each step you're still within your low-energy subspace."

The authors said their research applies to a large class of quantum systems and will be useful in simulating quantum field theories, which describe physical phenomena within their low-energy states.

Fast-forwarding of quantum systems bypasses the time-energy uncertainty principle

The other paper, "Fast-forwarding quantum evolution," a collaboration with Caltech's Shouzhen Gu—a former Los Alamos quantum computing summer school student—is published in Quantum. It shows three quantum systems in which a quantum simulation algorithm can run faster—and in some cases exponentially faster—than the limits suggested by the time-energy uncertainty principle.

"In quantum mechanics, the best precision that can be achieved when measuring a system's energy scales, in general, with the inverse of the duration of the measurement," said Somma.

"However, this principle does not apply to all quantum systems, especially those that have certain physical features," said Sahinoglu.

The authors showed that when this principle is bypassed, such quantum systems can also be simulated very efficiently, or fast-forwarded, on quantum computers.

36.Taiwan Sets Aside Millions in Budget to Promote Quantum Technology Workforce

by Matt Swayne
https://thequantuminsider.com/2021/12/13/taiwan-sets-aside-millions-in-budget-to-promote-quantum-technology-workforce/

Taiwan will invest heavily in quantum computing, Taiwan News is reporting and the premier is a believer in the promise of the technology.

The country will invest about NT$8 billion (US$288 million) for the development of quantum computing technology and building a quantum computing workforce, Premier Su Tseng-chan said recently.

Su said he believes quantum computing, along with artificial intelligence and big data, will play a pivotal role in shaping a smart society of the future, reports CNA, adding that he considers it a "next-generation computing technology" that would promote "revolutionary" changes to areas such as information security, finance, transportation and national defense.

Su also announced the country's first steps in pursuing this five-year — between 2022 and 2026 — initiative, according to Su.quantum computing. A task force has already been formed, which will rely on resources from technology and economic affairs departments as well as Academia Sinica.

The country will lean on its established technological strengths, such as chip manufacturing, to build the quantum ecosystem, said Su. The country's researchers are also adept at creating qubit control technology.

The Shalun Green Energy Technology Demonstration Site in Tainan will serve as the hub for the research and development of the technology.

37.Quantum computing nears a quantum leap

by Bryan Walsh
https://www.axios.com/quantum-computers-ibm-google-57070e8c-8bf6-40fd-83f2-b493db52f11e.html

A new class of powerful computers is on the brink of doing something important: actual useful work.

Why it matters: Quantum computers have the potential to solve unsolvable problems and break unbreakable encryption, but getting them to the point of reliability remains an enormous engineering challenge.

- But the companies — and countries — that figure out quantum will take the lead in a new era of computing.

What's happening: Quantum computers — which harness the weird and difficult physics of the quantum world — have experienced a number of notable improvements in recent weeks.

- In November, IBM unveiled its Eagle quantum processor, which packs 127 qubits — the quantum equivalent of the bits that drive classical computing — making it the first to break the 100-qubit barrier.

- This week, Quantinuum — a new quantum computing company created by the merger of software maker Cambridge Quantum and hardware manufacturer Honeywell Quantum Solutions — announced the world's first commercial product created solely by a quantum computer: a powerful encryption key generator.

- On Dec. 8, quantum computer maker IonQ — one of the few companies in the space to go public — announced plans to use barium ions as qubits in its systems, which president and CEO Peter Chapman says will improve the stability and reliability of its quantum computers.

By the numbers: The global quantum computing market is currently valued at $490 million, with 21.9% annual growth, and is projected to be worth nearly $1 billion by 2024, according to Bob Sorensen, chief analyst for quantum computing at Hyperion Research.

- "Hardware is hard, and it takes time for the engineering to advance from fundamental devices to useful devices," said William Oliver, director of the Center for Quantum Engineering at MIT, at this week's Q2B Practical Quantum Computing Conference.

- "But that is happening as quantum transitions from lab curiosity to technical reality."

How it works: Classical computers, from the smallest device to the most powerful supercomputer, do their calculations through the binary manipulation of bits, which can be in only two states: on or off, 1 or 0.

- Quantum computers use the quantum state of an object to produce qubits. The complex math behind these qubits can be plugged into special algorithms to do calculations that would be practically impossible for a classical computer to perform — a quality known as quantum advantage or supremacy.

- A working quantum computer could theoretically break the internet's most secure cryptography, solve impossibly complex logistical and optimization challenges, or simulate matter and chemistry on an incredibly precise scale.

- "We can do what's done now better and faster, and we'll be able to do things that can't be done at all right now," says Paul Lipman, president of quantum computing at hardware maker ColdQuanta.

The catch: More qubits should mean more powerful quantum computers, which is why hardware makers frequently tout the qubit totals on their latest models. For the machines to do useful work, they need to keep those qubits in a particular quantum state called a superposition as long as possible.

- But qubits are "highly sensitive," says IBM"s Jerry Chow, and slight variations of temperature or vibrations can cause them to lose their quantum state in a process called decoherence, turning qubits into boring old bits.

- Hardware makers face the challenge of building quantum computers that can add qubits without losing coherence, while software makers need to devise algorithms that can get the most out of what the machines can do.

- As a result, quantum computers can feel like a throwback to the early days of classical computing, with hardware makers pursuing multiple directions — trapped ions, neutral atoms, quantum annealing, silicon photonics — each of which might have different advantages for different applications.

- Oliver compared the current state of quantum computers to the Wright Brothers' first plane. "It was a key milestone in flight," he said, "but it wasn't like the next day we all went out and bought airplane tickets."

Between the lines: Even at this nascent stage, though, corporate customers are accessing quantum computers — usually through the cloud — to solve actual business problems.

- Quantum software makers like Zapata Computing and Multiverse Computing work with financial companies to better price derivatives and detect fraud.

- "Quantum advantage to me isn't about how we solve a problem," says Christopher Savoie, CEO and founder of Zapata. "It's how we use quantum to reduce your bottom line costs."

The bottom line: Improvement in computing power is what drives growth in the modern, digital economy. It's still very early days for quantum, but as both the hardware and software advance, the results could be extraordinary.

38.PASQAL Announces Quantum Computing Collaboration With Nvidia

by Nicolas Proust
https://thequantumhubs.com/pasqal-announces-quantum-computing-collaboration-with-nvidia/

QPASQAL today announced a collaboration with NVIDIA to build a Quantum Computing Center of Excellence, featuring a cluster of 10 NVIDIA DGX A100 systems with NVIDIA InfiniBand networking to enhance its portfolio of solutions.

PASQAL, a member of the NVIDIA Inception program which nurtures cutting-edge startups, will offer powerful quantum computing tools, supercharged by NVIDIA accelerated computing, to its customers across the entire value chain. In addition to broadening the spectrum of applications available, this cluster provides added technical capabilities for PASQAL's emulation system, which is based on its open-source library, Pulser. Pulser will be available via the cloud in early 2022.

Additionally, PASQAL will use the NVIDIA cuQuantum software development kit to further optimize the company's development operations. NVIDIA cuQuantum consists of libraries and tools designed to accelerate quantum computing workflows. PASQAL's developers will use cuQuantum to accelerate quantum circuit simulations based on state vector and tensor network methods by orders of magnitude.

"We are truly excited about this collaboration with NVIDIA. Our Quantum Computing Center of Excellence will enrich our emulation capabilities and is also part of our commitment to offer end users the best possible tools across the entire value chain," said **Loïc Henriet, CTO of Pasqal**.

"Quantum computing is helping researchers simulate complex phenomena for scientific discovery and address problems including optimization, drug discovery and machine learning.", said **Christophe Legrand, head of France Enterprise Computing at NVIDIA.** "PASQAL's Quantum Computing Center of Excellence, featuring NVIDIA DGX systems, will enable the simulation of tens of atomic qubits in 2D and 3D arrays to develop tools that will foster the development of industrial applications and can help advance scientific discovery."

39.Crucial leap in error mitigation for quantum computers

by Monica Hernandez and William Schulz
https://phys.org/news/2021-12-crucial-error-mitigation-quantum.html

Researchers at Lawrence Berkeley National Laboratory's Advanced Quantum Testbed (AQT) demonstrated that an experimental method known as randomized compiling (RC) can dramatically reduce error rates in quantum algorithms and lead to more accurate and stable quantum computations. No longer just a theoretical concept for quantum computing, the multidisciplinary team's breakthrough experimental results are published in Physical Review X.

The experiments at AQT were performed on a four-qubit superconducting quantum processor. The researchers demonstrated that RC can suppress one of the most severe types of errors in quantum computers: coherent errors.

Akel Hashim, AQT researcher, involved in the experimental breakthrough and a graduate student at the University of California, Berkeley explained: "We can perform quantum computations in this era of noisy intermediate-scale quantum (NISQ) computing, but these are very noisy, prone to errors from many different sources, and don't last very long due to the decoherence—that is, information loss—of our qubits."

Coherent errors have no classical computing analog. These types of errors are systematic and result from imperfect control of the qubits on a quantum processor, and can interfere constructively or destructively during a quantum algorithm. As a result, it is extremely difficult to predict their final impact on the performance of an algorithm.

Although, in theory, coherent errors can be corrected or avoided through perfect analog control, they tend to worsen as more qubits are added to a quantum processor due to "crosstalk" among signals meant to control neighbouring qubits.

First conceptualized in 2016, the RC protocol does not try to fix or correct coherent errors. Instead, RC mitigates the problem by randomizing the direction in which coherent errors impact qubits, such that they behave as if they are a form of stochastic noise. RC achieves this goal by creating, measuring, and combining the results of many logically-equivalent quantum circuits, thus averaging out the impact that coherent errors can have on any single quantum circuit.

"We know that, on average, stochastic noise will occur consistently at the same average error rate, so we can reliably predict what the results will be from the average error rates. Stochastic noise will never impact our system worse than the average error rate—something that is not true for coherent errors, whose impact on algorithm performance can be orders of magnitude worse than their average error rates would suggest."

Hashim used the analogy of the signal-to-noise ratio in astronomy to compare the impact of coherent errors versus stochastic noise in quantum computing. The longer a telescope operates, the more the signal will grow with respect to the noise, because the signal will coherently build upon itself, whereas the noise—being incoherent and uncorrelated—will grow much more slowly.

Coherent errors in quantum algorithms can build upon themselves through constructive interference and often grow faster than stochastic noise. However, the experimental demonstration of RC showed that coherent errors in quantum algorithms can be controlled to grow at a much slower rate.

The AQT team collaborated closely with the original creators of the protocol, Joseph Emerson and Joel Wallman, who co-founded the company Quantum Benchmark, Inc. (recently acquired by Keysight Technologies) to tackle the problem of benchmarking and mitigating errors in quantum computing systems.

"Not having to design the software ourselves to perform the RC protocol ultimately saved us a lot of time and resources and freed us to focus on the experimental work," Hashim said.

By bringing in researchers and partners from across the quantum information science community in the United States and the world, AQT enables the exploration and development of quantum computing based on one of the leading technologies, superconducting circuits.

"RC is a universal protocol for gate-based quantum computing, which is agnostic to specific error models and hardware platforms," Hashim described. "There are many applications and classes of algorithms out there that may benefit from the RC. Our collaborative research demonstrated that RC works to improve algorithms in the NISQ era, and we expect it will continue to be a useful protocol beyond NISQ. It is important to have this successful demonstration in our toolbox at AQT. We can now deploy it on other testbed user projects."

40.Winners announced in the BMW Group Quantum Computing Challenge

by James Goeders and Martin Schuetz
https://aws.amazon.com/blogs/quantum-computing/winners-announced-in-the-bmw-group-quantum-computing-challenge/

The four winning teams of the BMW Quantum Computing Challenge were announced this morning at the annual Q2B conference in Santa Clara, California. The challenge, focused on discovering potential quantum computing solutions for real-world use cases, was a collaboration between the BMW Group and the Amazon Quantum Solutions Lab Professional Services team.

"We at the BMW Group are convinced that future technologies such as quantum computing have the potential to make our products more desirable and sustainable," said Dr. Peter Lehnert, Vice President BMW Group Research and New Technologies Digital Car. "We have succeeded in reaching the global

quantum computing community with our crowd-innovation approach and enthusing them about automotive use cases. We look forward to continuing to work with the winners."

BMW Group Quantum Computing Challenge Use Cases

The BMW-AWS team selected four use cases for the competition: pre-production vehicle configuration, material deformation in production, vehicle sensor placement, and machine learning for automated quality assessment. Challenge participants were given AWS credits to use on Amazon Braket where they had access to available QPUs from D-Wave, IonQ, and Rigetti, and also quantum circuit simulators.

Use Case: Pre-Production Vehicle Configuration: One QuBit eNTiTy

The goal of this use case was to perform a maximum number of required tests on a minimum number of vehicles, while accounting for buildability and scheduling constraints to optimize pre-production vehicle testing. The winning team of One QuBit eNTiTy (comprised of researchers from 1Qbit, NTT Research, and NTT Data) provided a comprehensive solution strategy, including both hybrid (quantum-classical) approaches with near-term impact, and also a long-term quantum-native solution for fault-tolerant quantum hardware. The latter relies on a combination of the Duerr-Høyer algorithm for Quantum Minimum Finding and Quantum Amplitude Amplification, for which One QuBit eNTiTy worked out a thorough scaling analysis. Complementary to this long-term approach, the One QuBit eNTiTy team also developed a native and highly modular hybrid optimization technique, utilizing a fast classical or quantum MaxSAT solver as a sub-solver. The solution also comes with plugins for quantum-inspired devices, such as coherent Ising machines. Preliminary numerical experiments show promising results worth further investigation.

Use Case: Simulation of Material Deformation in Production: Qu&Co

This use case involved the development of novel quantum algorithmic approaches to model and numerically simulate material deformation, as relevant for the accurate prediction of material properties in the pre-production phase of vehicle component manufacturing. Mathematically this problem can be generalized to solving non-linear partial differential equations. The winning team from quantum computing startup Qu&Co provided a detailed, NISQ-ready solution strategy to this use case, based on differentiable quantum circuits. Moreover, the Qu&Co team included in their proposal promising benchmark comparisons to exact results, and results based on classical neural networks.

Use Case: Vehicle Sensor Placement: Accenture

Modern vehicles come with sensors to help provide safety and convenience to drivers. Vehicles need these sensors to gather data from as large a portion of their surroundings as possible, but each additional sensor adds costs. The goal of this use case was to optimize the positions of sensors to allow for maximum coverage while keeping the required number of sensors as low as possible. The Accenture team provided a holistic workflow for prototyping, from user input all the way to the final result, involving a detailed pipeline for (i) the definition of the input data, (ii) pre-processing steps, (iii) optimization of the underlying MaxCover problem and (iv) visualization of the results with an advanced

sensor distribution visualization app. For the actual optimization problem, the Accenture team developed a general framework including four classes of algorithmic approaches. While classical custom algorithms delivered the best results today, the framework from the Accenture team comes with plugins for quantum methods to be elaborated in the future.

Use Case: Machine Learning for Automated Quality Assessment: QC Ware

Manufacturers today heavily use classical deep-learning algorithms to assess vehicle parts for cracks and scratches caused by the metal-forming process, based on the successful segmentation and classification of imperfections. In this use case, the goal was to explore novel quantum or hybrid classical-quantum machine learning (QML) approaches that have the potential to provide more efficient training with higher accuracy to help improve the automated quality assessment of vehicles. The winning team from QC Ware provided a comprehensive solution involving three novel quantum algorithms for automated image classification. They were based on improvements for linear algebra routines to implement faster convolutional products compared to classical counterparts. In addition to complexity-theoretic arguments, the team presented extensive classical numerical simulations on two different image datasets. While today QML will not be able to solve this classification task better than established classical methods, the work from the QC Ware team allows us to understand where and how we can use quantum to enhance deep learning techniques in the future.

About the competition

Submissions were received from more than 70 teams globally, spanning from quantum software startups to enterprise companies. The jury evaluated the submissions for comprehensibility, feasibility, scalability, innovation, and benefit for the BMW Group. From the initial submissions, 15 finalists were selected before the final selection of the four winners.

41.China could beat US in AI, 5G, quantum computing: Harvard report

https://www.theweek.in/news/sci-tech/2021/12/08/china-could-beat-us-in-ai-5g-quantum-computing-harvard-report.html

A report by Harvard University has highlighted the massive advances China has made in multiple fields of cutting-edge technology.

The report by the Belfer Center of Harvard was published on Tuesday. Warning about the prevailing attitudes towards China, the report points out China's massive growth in manufacturing had enabled advances in research and development.

"It has displaced the US as the world's top high-tech manufacturer, producing 250 million computers, 25 million automobiles, and 1.5 billion smartphones in 2020," the report noted.

It warned China was already number one in some areas, while it could overtake the US in others, based on their current trajectories.

Artificial intelligence

The Harvard report reiterated the view of Eric Schmidt, the former CEO of Google, that China is now a "full-spectrum peer competitor" of the US in artificial intelligence.

Referring to key sectors of artificial intelligence, the report stated, "In speech technology, Chinese firms are beating American firms in every language, including English. The world's top voice recognition startup, China's iFlytek, has 700 million users, almost twice the number of people who speak to Apple's Siri. In financial technology (fintech), WeChat Pay's 900 million Chinese users vastly outnumber Apple Pay's 44 million in the US. While two-thirds of Americans still rely on credit cards, 90 percent of urban Chinese primarily use mobile payments, spending $150 on mobile platforms for every dollar Americans spend—in total, $42 trillion in 2020."

The Harvard report explained the importance of these numbers. It noted the spending "generates a treasure trove of granular data about individual consumer behaviour that can be used to develop other fintech applications, such as AI-driven assessments of individuals' credit-worthiness."

The report warned the US had "conceded the race" in facial recognition technology due to privacy concerns.

Referring to new areas of AI, the report described deep learning as the "hottest subfield". It noted, "China has six times more patent publications than the United States [in deep learning]. And according to the authoritative assessment of the Allen Institute for Artificial Intelligence, the United States will fall to second in the top 1% of most-cited AI papers by 2025."

5G

The report acknowledged China was the single largest 5G market in the world, accounting for 87 per cent of the 5G connections in the world at the end of 2020.

The report noted "nearly all key indicators support projections that China will dominate the 5G future. By the end of 2020, China had 150 million 5G users to America's 6 million; 700,000 5G base stations to America's 50,000; 460 MHz of licensed mid-band spectrum to America's 70 MHz; and 300 Mbps in average 5G speeds to America's 60 Mbps. Of the five major 5G equipment providers, two are Chinese; zero are American."

China was mindful of the competitive edge the US held in research and envelopment in 5G, standards and applications. "Recognising the value of 5G standards and fueled by high R&D budgets, Chinese companies are aggressively expanding their influence at standards bodies—and eroding America's. Huawei leads in shares of 5G patent families granted by the U.S. and European patent offices and in approved 5G technical contributions to 3GPP.," the report said.

The report warned the US would be at a disadvantage for future 5G applications given its lack of a robust national infrastructure.

"China is already pioneering cutting-edge 5G applications, including smart factory systems, digital twins for industrial applications, and the world's first 5G-enabled remote surgery," the report said.

Quantum computing

The Harvard report argued that China was catching up, and in some cases had overtaken the US in some fields of quantum information science (QIS), which includes quantum computing, quantum communication and quantum sensing. China currently spends four times more than the US on QIS.

"China has also demonstrated the ability to rapidly turn R&D into operational supremacy. In December 2020, only one year after Google's 53-qubit Sycamore superconducting quantum computer achieved quantum supremacy, China reached the same milestone. That month, a photonic quantum computer created by the University of Science and Technology of China reached quantum supremacy '10 billion times faster' than Google, for certain calculations in physics," the report noted.

Referring to quantum communication, the report said, "Edward Snowden's 2013 leaks revealing U.S. covert information gathering capabilities in China galvanised Beijing to accelerate progress in quantum communication—the 'gold standard' for security. As a result, in 2018 China registered over four times more patents than the US In quantum communication and cryptography (517 to 117)."

Warning about the strategic impact of these advances, the report said, "One expert expects Chinese government and military communications will go black in as little as two to three years, meaning the U.S. would no longer be able to listen in."

Semiconductors

While the US retains its dominance in semiconductors, its position has been eroded by underinvestment. On the other hand, "The Semiconductor Industry Association projects that over the next decade, China will develop 40% of new global capacity and become the world's largest semiconductor manufacturer, with 24% market share."

Biotechnology and green technology

The report highlights Chinese advances in biotechnology, an area where the US has traditionally been the market leader. China has made significant advances in basic and high-end research, pharmaceuticals and therapeutics.

While the US has been the primary inventor of many green technologies, China "has taken the lead in manufacturing and deploying those technologies, allowing it to dominate multiple links of the green energy supply chain".

The report noted, "China has sprinted ahead of the US and other countries to dominate the key links of the green tech supply chain, including equipment manufacturing, raw materials and energy storage.

Exploiting its status as the workshop of the world, China is now the dominant manufacturer of equipment for generating renewable energy. From producing less than 1% of solar panels in 2000, China now supplies 70% of solar panels globally. By comparison, in a stunning reversal, America's share fell from 30% in 2000 to less than 1% today. Four of the world's top ten wind turbine producers are Chinese and control 40% of the global market, versus 12% for the US."

The report predicts that by 2028, China will be making nearly six EVs for each one the US makes.

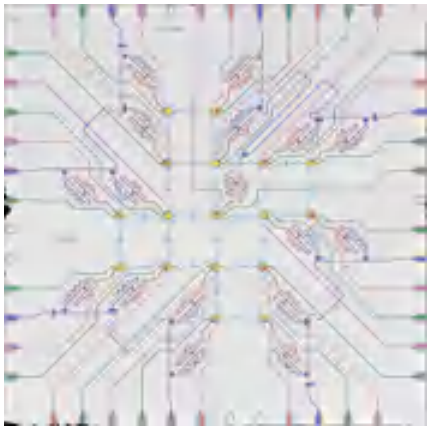
42.Our Team at ETH Zurich Realized Full Error Correction in a Quantum Processor

by Andreas Wallraff
https://www.linkedin.com/pulse/our-team-eth-zurich-realized-full-error-correction-quantum-wallraff/

Quantum error correction is a key ingredient for constructing fault-tolerant quantum information processors which will be able to execute complex quantum algorithms without being limited by unavoidable decoherence or control inaccuracies.

An approach which is know to be very resilient to errors in the physical qubits and their control is known as the surface code.

Using 17 superconducting qubits (yellow structures in image) we have realized such a surface code in

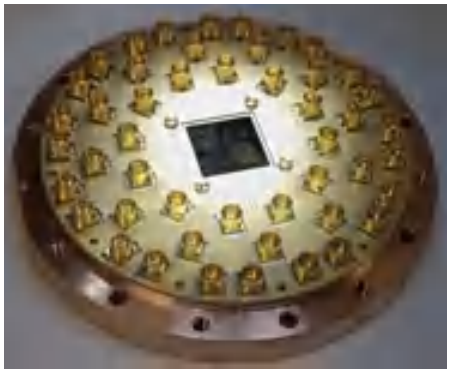


a single device. Nine physical qubits are used to encode the quantum information in an error-protected logical qubit. Eight qubits are used to detect the occurrence of two types of errors in the system: bit-flip errors and phase-flip errors, where the latter occur only in quantum computers and the former occur both in conventional and quantum computers. The device was designed at ETH Zurich by

Francois Swiadek and the team at the Quantum Device Lab and manufactured in the ETH Zurich clean-room facilities **FIRST** and **BRNC**.

The 17-qubit quantum circuit is mounted in a printed circuit board which allows for 48 control signals to be applied to the device on nanosecond time scales. On the photo you can make out the individual microwave lines leading up to the qubits. The photo was taken at the Quantum Device Lab of ETH Zurich by Christian Kraglund Andersen, who now runs his **own lab** as an Assistant Professor at TU Delft.

The quantum processor is operated at only a few thousands of a degree above the absolute zero of temperature in a cryogenic system. The base system is supplied by **Bluefors** but the side-loading wiring trees and all sample mounts have been conceived and designed by our Quantum Device Lab at ETH Zurich.



With an incredible team at our Quantum Device Lab at ETH Zurich and collaborators at Sherbrooke led by Alexandre Blais and with Markus Mueller RWTH Aachen we have realized fast and repeated quantum error correction in a distance three surface code.

This nice photo of part of the ETH team with Christopher Eichler, Nathan Lacroix, Sebsatian Krinner and I was taken on a weekend in early December in the hall way of our lab on the ETH Hoenggerberg Campus.

43.Honeywell-Backed Company To Sell Super Secure Quantum Encryption Key

by Jane Lanhee Lee
https://cio.economictimes.indiatimes.com/news/corporate-news/honeywell-backed-company-to-sell-super-secure-quantum-encryption-key/88143586

Quantum computer software firm Cambridge Quantum said on Tuesday it was launching a platform that can generate super secure cryptographic keys and sell them as a commercial product.

The UK-based startup this year became a wholly owned subsidiary of Quantinuum, a quantum computer hardware and software company in which Honeywell International Inc has a 54% stake.

Cambridge Quantum uses the quantum computer to generate a particularly random encryption key, said its head of cybersecurity Duncan Jones in an interview with Reuters.

Quantum computers can generate a more random encryption key than classical computers which makes them more secure and less vulnerable to cyber attacks, he said.

Cambridge Quantum said it would target its "Quantum Origin" service to financial services firms and cybersecurity firms before expanding it to other high priority sectors, such as telecommunications, energy, manufacturing, defense and government.

"We have been working for a number of years now on a method to efficiently and effectively use the unique features of quantum computers in order to provide our customers with a defense against adversaries and criminals now and in the future once quantum computers are prevalent," Ilyas Khan, CEO of Quantinuum and founder of Cambridge Quantum said in a statement.

"Quantum Origin gives us the ability to be safe from the most sophisticated and powerful threats today as well threats from quantum computers in the future."

Quantum computers are based on quantum bits, or qubits, that can be set to one and zero at the same time, creating exponentially more paths than classical computers whose bits are either ones or zeros. Researchers believe quantum computers could operate millions of times faster than today's advanced supercomputers.

44.Quantum Technology And Its Impact On Security In Mobile Networks

by Erik Ekudden
https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/ensuring-security-in-mobile-networks-post-quantum

The quantum technology of the future may have the potential to break some of the cryptography that provides security in today's mobile networks. While the risk is only theoretical at present and there is no way of knowing for certain if crypto-breaking quantum computers will ever actually exist, I encourage all communication service providers to prepare for that possibility. With the ability to decrypt communication, forge certificates and install fraudulent firmware updates, a quantum attacker could do enormous damage.

This article begins with a concise overview of the risks posed by quantum technology and goes on to explore the post-quantum cryptography solutions currently being standardized by organizations such as the US National Institute of Standards and Technology and the Internet Engineering Task Force.

While today's systems will remain secure against crypto-breaking quantum computers for many years to come, they do present a serious potential risk further into the future. To address this risk, new post-quantum algorithms that can easily be added to existing equipment and protocols are already in the final stages of standardization.

Over the last 50 years, cryptography has evolved from its military and diplomatic origins to become a rich and widely-used tool to create complex cryptographic solutions for a multitude of applications. In the ICT industry, for example, an efficient combination of symmetric and public-key (asymmetric) cryptography is critical to the security of virtually every product, service and interface in use today.

Modern critical infrastructure such as 5G is implemented with zero trust principles where cryptography is used for confidentiality, integrity protection, and authentication on many of the logical layers of the network stack, often all the way from device to software in the cloud[3]. The cryptographic solutions in use today are based on well-understood primitives, provably secure protocols and state-of-the-art implementations that are secure against a variety of side-channel attacks.

The first signs of a serious quantum challenge to modern cryptography arose in 1994, when the mathematician Peter Shor proved that quantum computers can efficiently factor large integers and solve the discrete logarithm problem, which is believed to be intractable on ordinary computers. Unfortunately, Shor's result also showed that if sufficiently large and robust quantum computers can be built, then today's public-key cryptography – which relies on the intractability of these problems – will be broken.

There are multiple public engagements in industry and academia to build quantum computers at present, but the gap between today's quantum computers and ones that could threaten current public-key cryptography is huge. It is believed that the ability to break today's public-key cryptography with Shor's algorithm would require millions of so-called qubits – the quantum equivalents of bits in ordinary computers. Today's quantum computers typically have a maximum of about 100 qubits and they are not as robust as they would need to be to execute Shor's algorithm.

While the future progress of robust quantum computers is complex and uncertain, it should not be judged on simple metrics such as qubit-count alone. Assuming a Moore's law type of growth in qubit count, the scaling from 100 qubits to millions of qubits would take 25-30 years. Recent claims of researchers reaching quantum supremacy do not tell us anything substantial about the speed at which the gap is closing between today's quantum computers and the hypothetical machines that could threaten public-key cryptography.

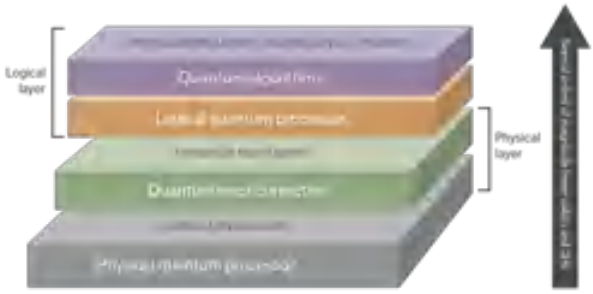
Risks presented by quantum technology

Nobody knows if large-scale, robust quantum computers capable of attacking public-key cryptography – sometimes called Cryptographically Relevant Quantum Computers (CRQCs) – will ever be built. A 2019 estimate by a committee of experts said that the emergence of a CRQC during the next decade

3 Ericsson Technology Review, Zero trust and 5G – Realizing zero trust in networks, May 2021, Olsson, J.; Shorov, A.; Abdelrazek, L.; Whitefield, J.

would be highly unexpected[4]. The committee also pointed out that there are no known applications for the intermediate medium-scale quantum computers that may appear in the coming years.

For most types of problem solving, quantum computers are much slower than ordinary computers, as the quantum error correction decimates the clock speed and number of usable qubits with several orders of magnitude, as shown in Figure. As a result, quantum computers are not general-purpose super computers, but rather potential special-purpose machines for physics simulations and certain problems that require clever quantum algorithms.



Some commentators have argued that the development of quantum computing could lose momentum due to a lack of short-term applications or if its progress is too slow[5]. Nonetheless, as the consequences of success would be so severe from a security point of view, anyone who uses public-key cryptography such as RSA and elliptic curve cryptography (ECC) should start preparing now for the possibility that such large-scale machines could someday be built.

After all, a quantum attacker could not only decrypt communication, but also forge certificates and install fraudulent firmware updates. This would completely break the security of most consumer electronics, enterprise networks, the industrial Internet of Things and critical infrastructure. Even worse, information encrypted using public-key cryptography today could be recorded by attackers and used for attacks in the future when large-scale robust quantum computers potentially exist.

Fortunately, an alternative is already available for very long-lived signature keys such as those used in firmware updates. Stateful hash-based signatures have well-understood security, and have already been standardized by the Internet Engineering Task Force (IETF) and the US National Institute of Standards and Technology (NIST)[6]. There is a serious limitation to stateful hash-based signatures, however. Because they are stateful, they are only suitable for very specific applications.

.
.
.

4 NAP, Quantum Computing: Progress and Prospects, 2019

5 IEEE Spectrum, The case against quantum computing, November 15, 2018, Dyakonov, M

6 NIST, SP 800-208, Recommendation for Stateful Hash-Based Signature Schemes, October March 2020

Ericsson's role

Ericsson is engaging in the NIST PQC standardization and the PQC discussions in the IETF, 3GPP and ETSI, and will remain active when standards used in 5G such as TLS (Transport Layer Security), IKEv2 (Internet Key Exchange version 2), X.509, JOSE (JavaScript Object Signing & Encryption) and 5G SUCI (Subscription Concealed Identifier) are updated with the finalized NIST algorithms. While standards may be updated to support the new NIST PQC algorithms, it remains to be seen at what speed our current public-key cryptography is deprecated. This may, in part, depend on the progress in building quantum computers in the coming years. There is a balance between prudent preparations for switching to PQC and making sure that the investment in implementing PQC will be a long-term secure and good choice.

One way in which we are preparing Ericsson's products is by aligning with practices in the NIST Migration to Post-Quantum Cryptography project[7]. One key is crypto agility – the ability to upgrade cryptography and be prepared for the larger public keys used in PQC, for example. The US National Security Agency's (NSA's) Commercial National Security Algorithm (CNSA) cryptography suite is used to protect information in national security systems (NSSs)[8]. The CNSA suite is still not quantum-resistant, and information in NSSs may need protection for decades. This indicates that the NSA feels confident that large-scale robust quantum computers will not be a threat for decades to come.

For the most part, standardization organizations, governments and industries are waiting for the final outcome of the NIST PQC standardization before they take action. The NSA became the exception recently when it announced its plans to add support in the CNSA suite for some of the lattice-based proposals at the end of the third round of the NIST standardization, planned for early 2022.

Post-quantum cryptography algorithm deployment

The initial deployment of the new PQC algorithms may be done in combination with current public-key cryptography so that, for example, an attacker would need to break both conventional elliptic curve Diffie-Hellman KEMs and one of the new PQC KEMs to learn an established session key in a communication protocol. For the most part, the migration to PQC is an algorithm update just like the previous updates from DES (Data Encryption Standard) to AES (Advanced Encryption Standard) and SHA (Secure Hashing Algorithm)-1 to SHA-2, but the larger sizes and slightly limited properties may require changes in protocols and application programming interfaces. The communication overhead of the new algorithms could lead to packet fragmentation in network communication, for example.

Quantum impact on symmetric cryptography

In 1996, Shor's result was complemented by an algorithm developed by the computer scientist Lov Grover, which showed that quantum computers could search through the possible inputs to a black-box function to find an input that gives a sought output. While Grover's algorithm can do this in much fewer evaluations of the black-box function than any ordinary algorithm, it is still very slow compared

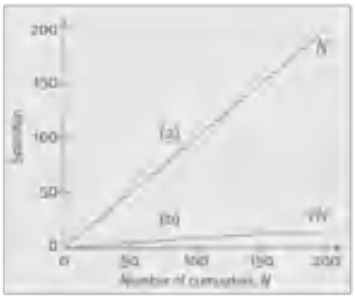
---

7 NIST, Migration to Post-Quantum Cryptography, August 2021, Barker, W; Souppaya, M; Newhouse, W

8 NSA, Commercial National Security Algorithm Suite

with Shor's quantum algorithm. (The meaning of black box in this context is that Grover's algorithm does not rely on any internal structure of the function – it is a generic method.)

In theory, an attacker with a quantum computer can use Grover's algorithm to break the symmetric cipher AES-128 through a quantum computation that consists of 264 serial AES-128 encryptions. Each such AES-128 encryption in turn consists of approximately 211 serial quantum gates. This gives a total serial computation of length 275 quantum gates. However, the quantum gates can introduce errors, and further overhead piles up from quantum error-correction. What all this means in practice is that the attacker must split up the computation over multiple quantum computers. Since Grover's algorithm does not parallelize efficiently, as illustrated in Figure, the use of 100 quantum computers would only speed up the computation by a factor of 10.



Considering all this, Grover's algorithm does not pose any apparent threat to symmetric cryptography. Some years ago, there was a common conception that Grover's algorithm required symmetric key sizes to be doubled – requiring use of AES-256 instead of AES-128. This is today considered a misconception – NIST, for example, now states that AES-128 will likely remain secure for decades to come, despite Grover's algorithm[9].

In fact, one of the security levels in the NIST PQC standardization is equivalent to that of AES-128. This means that NIST thinks it is relevant to standardize parameters for PQC that are as strong under quantum attacks as AES-128. There could, of course, be other reasons why a longer key is needed, such as compliance, and using a longer key only has a marginal effect on performance.

In summary, our most important symmetric cryptographic tools (AES, SNOW 3G, SHA2, SHA3 and so on) remain secure against quantum computers as they are. This also applies to the authentication, key generation, encryption and integrity in 3G, 4G and 5G that rely purely on symmetric cryptography.

.
.
.

Conclusion

While we do not expect quantum computers with the ability to attack current cryptography to emerge for many years to come, we strongly encourage communication service providers to start planning the process of migrating to post-quantum cryptography. With the support of vendors including Ericsson, standards-developing organizations such as the US National Institute of Standards and Tech-

9 NIST, Post-Quantum Cryptography

nology, the Internet Engineering Task Force and the 3GPP are working on new, post-quantum algorithms and updated protocols that can easily be added to existing equipment and interfaces. Currently in the final stages of standardization, these algorithms will be available in the next couple of years to help our industry mitigate potential future threats against mobile infrastructure and services.

45.Cambridge Quantum Launches Quantum Origin

https://cambridgequantum.com/quantum-origin-press-release/

Cambridge Quantum, the global leader in quantum software, and a wholly owned subsidiary of Quantinuum, the world's leading integrated quantum computing company, is pleased to announce that it is launching Quantum Origin – the world's first commercially available cryptographic key generation platform based on verifiable quantum randomness. It is the first commercial product built using a noisy, intermediate-scale quantum (NISQ) computer and has been built to secure the world's data from both current and advancing threats to current encryption.

Randomness is critical to securing current security solutions as well as protecting systems from the future threat of quantum attacks. These attacks will further weaken deterministic methods of random number generation, as well as methods that are not verifiably random and from a quantum source.

Today's systems are protected by encryption standards such as RSA and AES. Their resilience is based on the inability to "break" a long string from a random number generator (RNG). Today's RNGs, however, lack true, verifiable randomness; the numbers being generated aren't as unpredictable as thought, and, as a result, such RNGs have been the point of failure in a growing number of cyber attacks. To add to this, the potential threat of quantum attacks is now raising the stakes further, incentivising criminals to steal encrypted data passing over the internet, with a view to decrypting it later using quantum computers. So-called "hack now, decrypt later" attacks.

Quantum Origin is a cloud-hosted platform that protects against these current and future threats. It uses the unpredictable nature of quantum mechanics to generate cryptographic keys seeded with verifiable quantum randomness from Quantinuum's H-Series quantum computers, Powered by Honeywell. It supports traditional algorithms, such as RSA or AES, as well as post-quantum cryptography algorithms currently being standardised by the National Institute for Standards and Technology (NIST).

"We have been working for a number of years now on a method to efficiently and effectively use the unique features of quantum computers in order to provide our customers with a defence against adversaries and criminals now and in the future once quantum computers are prevalent," said Ilyas Khan, CEO of Quantinuum and Founder of Cambridge Quantum. He added "Quantum Origin gives us the ability to be safe from the most sophisticated and powerful threats today as well as threats from quantum computers in the future."

Duncan Jones, head of cybersecurity at Cambridge Quantum, said: "When we talk about protecting systems using quantum-powered technologies, we're not just talking about protecting them from future threats. From large-scale takedowns of organisations, to nation state hackers and the worrying potential of 'hack now, decrypt later' attacks, the threats are very real today, and very much here to stay. Responsible enterprises need to deploy every defense possible to ensure maximum protection at the encryption level today and tomorrow."

Quantum-enhanced keys on demand

With Quantum Origin, when an organisation requires quantum-enhanced keys to be generated, it can now make a call via an API. Quantum Origin generates the keys before encrypting them with a transport key and securely relaying them back to the organisation. To give organisations a high-level of assurance that their encryption keys are as unpredictable as possible, Quantum Origin tests the entire output from the quantum computers, ensuring that each key is seeded from verifiable quantum randomness.

These keys are then simple and easy to integrate within customers' existing systems because they're provided in a format that can be consumed by traditional cybersecurity systems and hardware. This end-to-end approach ensures key generation is on-demand and is capable of scaling with use, all while remaining secure.

Quantum Origin in practice

Quantum Origin keys should be used in any scenario where there is a need for strong cybersecurity. At launch, Cambridge Quantum will offer Quantum Origin to financial services companies and vendors of cybersecurity products before expanding into other high priority sectors, such as telecommunications, energy, manufacturing, defence and government.

The technology has already been used in a series of projects with launch partners. Axiom Space used Quantum Origin to conduct a test of post-quantum encrypted communication between the ISS and Earth – sending the message "Hello Quantum World" back to earth encrypted with post-quantum keys seeded from verifiable quantum randomness. Fujitsu integrated Quantum Origin into its software-defined wide area network (SDWAN) using quantum-enhanced keys alongside traditional algorithms.

46.Microsoft to Bring Rigetti Superconducting Quantum Computers to Azure Quantum

https://thequantumhubs.com/microsoft-to-bring-rigetti-superconducting-quantum-computers-to-azure-quantum/

Rigetti Computing, a pioneer in full-stack quantum computing, today announced a collaboration with Microsoft to provide Rigetti quantum computers over the cloud to users of Microsoft's Azure Quantum service. When the Rigetti system becomes available, it will be the largest quantum computer accessible on Azure Quantum. The two companies expect the integration to be completed and available to users in the first quarter of 2022.

Rigetti quantum computers use superconducting qubits, a technology approach shown to have faster execution times and greater scaling than other commercially available quantum computing technologies. These performance characteristics position Rigetti quantum computers to potentially help solve a broad range of valuable problems in areas like machine learning, drug discovery, clean energy, logistics optimization, and financial simulations.

"We're excited to bring the speed and scale of Rigetti quantum computers to the Azure Quantum marketplace," said Taryn Naidu, chief operating officer of Rigetti. "Microsoft has fostered an impressive community of quantum developers and researchers. Together, we can power a new generation of algorithms that chart the path toward quantum advantage."

"Rigetti's scalable approach to superconducting quantum computers will create new opportunities for the Azure Quantum development community," said Krysta Svore, General Manager of Microsoft Quantum. "We're working closely with Rigetti to deliver hybrid quantum-classical computing with the performance to tackle problems that were previously out of reach."

Azure Quantum developers will be able to program Rigetti computers using popular quantum software frameworks. This week at Q2B 2021 — the quantum computing industry's premier conference — Rigetti is demonstrating a quantum chemistry algorithm using QIR, Microsoft's quantum intermediate representation, running on a Rigetti quantum computer over the cloud. Rigetti and Microsoft are collaborating, as part of the QIR Alliance, toward a goal of enabling interoperability within the quantum ecosystem and reducing development efforts from all parties.

47."Hello Quantum World:" New cybersecurity service uses entanglement to generate cryptographic keys

by Veronica Combs
https://www.techrepublic.com/article/hello-quantum-world-new-cybersecurity-service-uses-entanglement-to-generate-cryptographic-keys/

Quantinumm's software company Cambridge Quantum announced a new way to provide cryptographic keys that uses Honeywell's H1, entanglement and an API. Quantum Origin can run on any quantum computer and is designed to integrate into existing cybersecurity solutions.

This new cloud-based method uses quantum entanglement to generate cryptographic keys and is based on verifiable quantum randomness, according to the company. The company generates the keys before encrypting them with a transport key and relaying them back to a customer.

Duncan Jones, head of cybersecurity at Cambridge Quantum, said Quantum Origin is kickstarting the quantum cybersecurity industry.

Ilyas Khan, CEO of Quantinuum and founder of Cambridge Quantum, said that the key generator was tested on Oxford Quantum's and IBM's quantum computers.

"At the moment, the best results have come from a trapped ion system but that could change tomorrow," he said. "The product is platform agnostic and could generate the key using any number of quantum computers that come online in the future."

Jones said that Cambridge Quantum's device-agnostic approach is what makes this service different from other attempts to use quantum computers for cybersecurity.

In a white paper about Quantum Origin, Cambridge Quantum describes device independence this way: "We can isolate the particular bit of quantum behaviour we are looking for and then make it available to other systems so that everyone can benefit and security can be increased across the board," he said.

> "In a fully device-independent (DI) protocol, only minimal assumptions are made about the physical device that executes the protocol. Instead, the device is treated as a black box, and the protocol simply provides inputs and interrogates the output from the device."

The product supports RSA and AES algorithms as well as the post-quantum cryptography algorithms being standardized by the National Institute for Standards and Technology. The service is priced per key generated for customers.

Jones said that the company has export controls in place to screen customers who want to use the service.

"As part of our customer onboard process, we do due diligence to make sure use cases and destination countries are all above board," he said.

Khan described Quantum Origin as a defensive technology as opposed to an adversarial one.

"We are focused on protecting the technology that creates the key, not selling it," he said. "We are selling the product created by that technology."

Cambridge Quantum will offer the new service to financial services companies and cybersecurity vendors initially and later to telecommunications, energy, manufacturing, defense and governments.

Encrypting data in space and over SDWANs

During a press call on Monday, leaders from two companies that have used these quantum keys explained their experiences with the new service.

Axiom Space used the service to send post-quantum encrypted messages between the International Space Station and Earth. The company's first quantum encrypted message sent from the ISS was "Hello Quantum World." Axiom chose Quantum Origin to protect data from in-space manufacturing, experiments, services and Department of Defense initiatives.

"If we can't secure our data, that hurts a really expensive asset that is floating out in space," David Zuniga said during the press call.

Axiom is building the infrastructure for low-Earth orbit operations and a commercial space station. The company plans to send humans into space in February 2022.

Khan said work done on the space station could be critically important to researchers now and in the future.

"We don't want people hacking into systems and harvesting data to use later," he said. "You're not just protecting against future attacks, you're protected today against the worst that the adversary can throw out."

In a proof-of-concept project, Fujitsu used the service in its software-defined wide area network using quantum-enhanced keys with traditional algorithms. Houton Houshmand, CTO and research lead at Fujitsu, said that the new keys will protect applications, edge routing and cloud infrastructure from cyber attacks.

"We are looking above the stack over the SD WAN to protect the security of data inside the application and address data security needs of the application as well," he said.

Growing concerns about standard encryption

A recent survey commissioned by Cambridge Quantum found that existing encryption methods may last only two more years. Dimensional Research conducted the survey for the quantum company in October and asked 600 cybersecurity professionals about these concerns. Sixty percent of respondents predict current encryption will be broken by 2023 by new and evolving technologies.

Only 21% said they were ready for this sea change in cybersecurity. Another 38% said they will be ready within the next two years. Unfortunately, only 20% of respondents said their organizations are allocating funds to address this challenge. An even smaller group — 13% — have purchased a solution to do so.

The survey also found that:

- 80% of respondents are worried that a quantum-powered attack could occur without warning
- 86% said they comply to regulations requiring critical data protections for an extended period

48.How the United States Is Developing Post-Quantum Cryptography

by Jeremy Hsu
https://spectrum.ieee.org/how-the-us-is-preparing-for-quantum-computings-threat-to-end-secrecy

When practical quantum computing finally arrives, it will have the power to crack the standard digital codes that safeguard online privacy and security for governments, corporations, and virtually everyone who uses the Internet. That's why a U.S. government agency has challenged researchers to develop a new generation of quantum-resistant cryptographic algorithms.

Many experts don't expect a quantum computer capable of performing the complex calculations required to crack modern cryptography standards to become a reality within the next 10 years. But the U.S. National Institute of Standards and Technology (NIST) wants to stay ahead by getting new cryptographic standards ready by 2022. The agency is overseeing the second phase of its Post-Quantum Cryptography Standardization Process to narrow down the best candidates for quantum-resistant algorithms that can replace modern cryptography.

"Currently intractable computational problems that protect widely-deployed cryptosystems, such as RSA and Elliptic Curve-based schemes, are expected to become solvable," says Rafael Misoczki, a cryptographer at the Intel Corporation and a member of two teams (named Bike and Classic McEliece) involved in the NIST process. "This means that quantum computers have the potential to eventually break most secure communications on the planet."

Misoczki was one of more than 250 registered attendees who signed up for the Second PQC Standardization Conference held at the University of California, Santa Barbara from 22 to 25 August. The event featured presentations from almost all of the teams working on 26 candidate algorithms, which were winnowed down from 69 first-round candidates.

NIST hopes these second-round candidates will evolve beyond mere proofs of concept and begin benchmarking tests. The stakes are high, given that a quantum computing breakthrough could threaten to undermine security for hundreds of billions of dollars in e-commerce alone—not to mention the trillions of dollars at risk in the broader digital economy. Still, many researchers have cautioned that NIST should take its time to evaluate the new class of candidates for post-quantum cryptography before selecting any finalists.

Meet the Quantum-Resistant Algorithms

The NIST process is considering algorithms that fall into two general categories, Misoczki explains. The first category includes key-establishment algorithms that enable two parties that have never met to agree on a shared secret. This category also includes public-key encryption algorithms—such as RSA and Elliptic Curve cryptography—that do the same thing, but are less efficient.

A second category involves algorithms for digital signatures that ensure the authenticity of data. Such digital signatures feature in code-signing applications that establish confidence that a program was created by the intended developer and not by a hacker.

Both categories require new algorithms based upon mathematical problems which even quantum computers couldn't crack. There are several approaches to post-quantum cryptography algorithms under consideration, and each has pros and cons. For example, "families such as code-based cryptography enjoy a long history of public scrutiny, while lattice-based cryptography offers very fast algorithms," Misoczki says.

The tradeoffs between each approach can have significant real-world implications for computing applications and devices. Lattice-based cryptography is even faster than modern cryptographic approaches such as RSA, but its bigger data size could make a difference if bandwidth is relatively scarce.

That's why it makes sense for NIST to standardize algorithms from several different approaches, says Vadim Lyubashevsky, a cryptography researcher at the IBM Zurich Research Laboratory in Switzerland and participant in the NIST process. "Even if we were sure they were all secure, no candidate is best in every area," Lyubashevsky says.

Much remains unknown about these candidate algorithms that will likely replace large parts of the world's infrastructure underpinning secure global communication, says Peter Schwabe, a computer security researcher at Radboud University in the Netherlands. More development and testing is needed to assess each algorithm's actual cryptographic security against the best possible attacks, measure its security-performance tradeoffs, develop techniques to implement the algorithms securely, and find things that can go wrong when deploying them.

"What seems quite clear by now is that the new schemes have massively different performance characteristics than the ones we use today and many have subtly different security properties," Schwabe says.

Cooperative Spirit vs. Competitive Streak

The NIST challenge has brought together both academic researchers focused on theoretical work and tech industry experts familiar with real-world performance needs and security demands. The agency initially described it as a "competition-like process," but seems eager to encourage a cooperative spirit among participants.

Some researchers have joined multiple teams working on different algorithms. For example, Lyubashevsky is a member of groups working on algorithms such as CRYSTAL-KYBER, CRYSTALS-DILITHIUM, and Falcon. Schwabe belongs to seven teams focused on specific algorithms: CRYSTALS-KYBER, CRYSTALS-DILITHIUM, Classic McEliece, NewHope, SPHINCS+, NTRU, and MQDSS.

Teams openly share frameworks and feedback on a single mailing list—an approach that has benefits and drawbacks. "Certain vocal and at times outright impolite personalities dominate the mailing list, causing others to hesitate to contribute their work or questions," wrote one anonymous participant in response to a NIST survey.

Most of the community seems dedicated to working together, says Misoczki, who has observed "more of a cooperative environment rather than a competitive situation" despite some differences of opinion.

Schwabe also described the community's cooperative spirit, but noted that some individuals seem to have more of a competitive streak. "Unfortunately, some participants are not that cooperative, and have a focus on pushing for 'their' (often patented) schemes rather than working as a community on finding the best scheme(s) to standardize and use in the future," Schwabe wrote in an email.

Some of the competing algorithms represent relatively minor variations on the same cryptographic approaches. Lyubashevsky suggested that NIST keep the participants focused on the common standardization goal by asking for specific cryptographic features that the agency wants in candidate algorithms.

"It would be good to say 'look, forget the names of people attached to these things, here are the features we want to see,'" Lyubashevsky says.

New Post-Quantum Cryptography Standards

NIST plans to draft standards for post-quantum cryptography around 2022. But researchers have urged the agency to avoid rushing the process of vetting all the candidate algorithms. Their anonymous feedback came from a NIST survey that was shared at the end of the Second PQC Standardization Conference in August.

"NIST should not be aiming to conclude the process and have standards written by 2022," wrote one survey respondent. "This is simply too fast to get proper answers…. Much more research is needed."

Another survey respondent proposed that "NIST should hold off creating any standard before 2025 and fund research efforts to look at all the candidates until that time," in order "to give researchers a chance to innovate."

One survey respondent painted an especially dire picture of the possible consequences of rushing ahead: "Attempting to end this process in just a couple more years is dangerous and could lead to disastrous results and/or a loss of perceived legitimacy of the process and output."

Many pointed to the need for more cryptanalysis to thoroughly investigate the possible weaknesses of each algorithm. One person urged NIST to sponsor more academic research at U.S. universities to further develop "the science of quantum cryptanalysis."

"The problem with cryptography in general is that cryptanalysis is such an unrewarding process," Lyubashevsky says. "Either you fail and no one knows that you tried and failed, or you succeed and you get your five minutes of fame, and then that algorithm that you wrote is never used again."

NIST may be partly counting on the idea that different teams will try to break each other's algorithms. But Lyubashevsky suggested that the agency should also look into requiring researchers to check another group's work, or perhaps make cryptanalysis part of the conditions for funding the theoretical work in developing the algorithms.

When Will Computers Crack Cryptography?

Nobody knows exactly when quantum computing will render modern cryptographic algorithms useless. One complication is that the first government or organization to develop a practical quantum computer could gain a lot by simply keeping quiet, breaking modern cryptography systems and hoovering up the world's secrets.

"I see a good chance that the first large universal quantum computers will be available only to government agencies who will not exactly advertise that they have such computing capabilities," Schwabe says. He sees a "realistic chance that within 20 years there will be quantum computers that break the cryptography we have in wide use today."

What cryptography researchers do know is that it can take a long time for the world's governments and industries to adopt the latest cryptographic standards. Even though Elliptic Curve Cryptography was first proposed in the late 1980s, much of the world still relies on older RSA cryptography that appeared in the late 1970s. That's why there is still some urgency behind NIST's standardization effort for post-quantum cryptography, even if practical quantum computing remains a few decades away.

"Predicting when large-scale quantum computers will become available is a hard question," Misoczki says. "On the other hand, the crypto community knows that transitioning crypto algorithms takes several years, even decades."

Luckily, forward-thinking organizations holding extremely sensitive data don't need to wait for the NIST standardization process to play out before taking steps to future-proof their systems. Instead, they could simply go ahead and adopt some of the candidate algorithms in the NIST process that have been published publicly online and are free to use.

"If you really have sensitive data, do it now, migrate yourself," Lyubashevsky says. "If you don't have such data, then I think it'd be good to wait five years and let the competition run its course to come up with a nice standard that most people are happy with."

As for those willing to wait, Lyubashevsky expressed confidence that cryptographers working together with NIST would be ready for a future with quantum computing.

"We'll definitely have post-quantum cryptography before quantum computers are ready," Lyubashevsky says. "I think if we take the next five years to really get the standards of post-quantum cryptography right, it's enough time for virtually every application."

49.The future of scientific research is quantum

by Rosa Di Felice, Anna Krylov, Marco Fornari, Marco Buongiorno Nardelli, Itay Hen and Amir Kalev
https://thenextweb.com/news/the-future-of-scientific-research-is-quantum-syndication

Over the past few years, the capabilities of quantum computers have reached the stage where they can be used to pursue research with widespread technological impact. Through their research, the Q4Q team at the University of Southern California, University of North Texas, and Central Michigan University, explores how software and algorithms designed for the latest quantum computing technologies can be adapted to suit the needs of applied sciences. In a collaborative project, the Q4Q team sets out a roadmap for bringing accessible, user-friendly quantum computing into fields ranging from materials science, to pharmaceutical drug development.

Quantum computing

Since it first emerged in the 1980s, the field of quantum computing has promised to transform the ways in which we process information. The technology is centered on the fact that quantum particles – such as electrons – exist in 'superpositions' of states. Quantum mechanics also dictates that particles will only collapse into one single measurable state when observed by a user. By harnessing these unique properties, physicists discovered that batches of quantum particles can act as more advanced counterparts to conventional binary bits – which only exist in one of two possible states (on or off) at a given time.

On classical computers, we write and process information in a binary form. Namely, the basic unit of information is a bit, which takes on the logical binary values 0 or 1. Similarly, quantum bits (also known as 'qubits') are the native information carriers on quantum computers. Much like bits, we read binary outcomes of qubits, that is 0 or 1 for each qubit.

However, in a stark contrast to bits, we can encode information on a qubit in the form of a superposition of logical values of 0 and 1. This means that we can encode much more information in a qubit than in a bit. In addition, when we have a collection of qubits, the principle of superposition leads to computational states that can encode correlations among the qubits, which are stronger than any type of correlations achieved within a collection of bits. Superposition and strong quantum correlations are, arguably, the foundations on which quantum computers rely on to provide faster processing speeds than their classical counterparts.

To realize computations, qubit states can be used in quantum logic gates, which perform operations on qubits, thus transforming the input state according to a programmed algorithm. This is a paradigm for quantum computation, analogous to conventional computers. In 1998, both qubits and quantum logic gates were realized experimentally for the first time – bringing the previously-theoretical concept of quantum computing into the real world.

Stalling advances

From this basis, researchers then began to develop new software and algorithms, specially designed for operations using qubits. At the time, however, the widespread adoption of these techniques in everyday applications still seemed a long way off. The heart of the issue lay in the errors that are inevitably introduced to quantum systems by their surrounding environments. If uncorrected, these errors can cause qubits to lose their quantum information, rendering computations completely useless. Many studies at the time aimed to develop ways to correct these errors, but the processes they came up with were invariably costly and time-consuming.

Unfortunately, the risk of introducing errors to quantum computations increases drastically as more qubits are added to a system. For over a decade after the initial experimental realization of qubits and quantum logic gates, this meant that quantum computers showed little promise in rivalling the capabilities of their conventional counterparts.

In addition, quantum computing was largely limited to specialized research labs, meaning that many research groups that could have benefited from the technology were unable to access it.

Improving accessibility

While error correction remains a hurdle, the technology has since moved beyond specialized research labs, becoming accessible to more users. This occurred for the first time in 2011, when the first quantum annealer was commercialized. With this event, feasible routes emerged towards reliable quantum processors containing thousands of qubits capable of useful computations.

Quantum annealing is an advanced technique for obtaining optimal solutions to complex mathematical problems. It is a quantum computation paradigm alternative to operating on qubits with quantum logic gates.

The availability of commercial quantum annealers spurned a new surge in interest for quantum computing, with consequent technological progress, especially fuelled by industrial capitals. In 2016, this culminated in the development of a new cloud system based on quantum logic gates, which enabled owners and users of quantum computers around the world to pool their resources together, expanding the use of the devices outside of specialized research labs. Before long, the widespread use of quantum software and algorithms for specific research scenarios began to look increasingly realistic.

At the time, however, the technology still required high levels of expertise to operate. Without specific knowledge of the quantum processes involved, researchers in fields such as biology, chemistry,

materials science, and drug development could not make full use of them. Further progress would be needed before the advantages of quantum computing could be widely applied outside the field of quantum mechanics itself.

Useful quantum simulations

Now, the Q4Q team aims to build on these previous advances – using user-friendly quantum algorithms and software packages to realize quantum simulations of physical systems. Where the deeply complex properties of these systems are incredibly difficult to recreate within conventional computers, there is now hope that this could be achieved using large systems of qubits.

To recreate the technologies that could realistically become widely available in the near future, the team's experiments will incorporate 'noisy intermediate-scale quantum' (NISQ) devices – which contain relatively large numbers of qubits, and by themselves are prone to environmental errors.

In their projects, the Q4Q team identifies three particular aspects of molecules and solid materials that could be better explored through the techniques they aim to develop. The first of these concerns the 'band structures' of solids – which describe the range of energy levels that electrons can occupy within a solid, as well as the energies they are forbidden from possessing.

Secondly, they aim to describe the vibrations and electronic properties of individual molecules – each of which can heavily influence their physical properties. Finally, the researchers will explore how certain aspects of quantum annealing can be exploited to realize machine-learning algorithms – which automatically improve through their experience of processing data.

Molecules and solids

As they apply these techniques, the Q4Q team predicts that their findings will lead to a better knowledge of the quantum properties of both molecules and solid materials. In particular, they hope to provide better descriptions of periodic solids, whose constituent atoms are arranged in reliably repeating patterns.

Previously, researchers struggled to reproduce the 'wave-functions' of interacting quantum particles within these materials, which relate to the probability of finding the particles in particular positions when observed by a user. Through their techniques, the Q4Q team aims to reduce the number of qubits required to capture these wave-functions, leading to more realistic quantum simulations of the solid materials.

Elsewhere, the Q4Q team will account for the often deeply complex quantum properties of individual molecules made up of large groups of atoms. During chemical reactions, any changes taking place within these molecules will be strongly driven by quantum processes, which are still poorly understood. By developing plugins to existing quantum software, the team hopes to accurately recreate this quantum chemistry in simulated reactions.

If they are successful in reaching these goals, the results of their work could open up many new avenues of research within a diverse array of fields – especially where the effects of quantum mechan-

ics have not yet been widely considered. In particular, they will also contribute to identifying bottlenecks of current quantum processing units, which will aid the design of better quantum computers.

Expanding into new fields

Perhaps most generally, the Q4Q team hopes that their techniques will enable researchers to better understand how matter responds to external perturbations, such as lasers and other light sources.

Elsewhere, widely accessible quantum software could become immensely useful in the design of new pharmaceutical drugs, as well as new fertilizers. By ascertaining how reactions between organic and biological molecules unfold within simulations, researchers could engineer molecular structures that are specifically tailored to treating certain medical conditions.

The ability to simulate these reactions could also lead to new advances in the field of biology as a whole, where processes involving large, deeply complex molecules including proteins and nucleic acids are critical to the function of every living organism.

Finally, a better knowledge of the vibrational and electronic properties of periodic solids could transform the field of materials physics. By precisely engineering structures to display certain physical properties on macroscopic scales, researchers could tailor new materials with a vast array of desirable characteristics: including durability, advanced interaction with light, and environmental sustainability.

Training a new generation

If the impacts of the team's proposed research goals are as transformative as they hope, researchers in many different fields of the technological endeavour could soon be working with quantum technologies.

Such a clear shift away from traditional research practices could in turn create many new jobs – with required skillsets including the use of cutting-edge quantum software and algorithms. Therefore, a key element of the team's activity is to develop new strategies for training future generations of researchers. Members of the Q4Q team believe that this will present some of the clearest routes yet towards the widespread application of quantum computing in our everyday lives.

50.Mozilla patches critical "BigSig" cryptographic bug: Here's how to track it down and fix it

by Paul Ducklin
https://nakedsecurity.sophos.com/2021/12/03/mozilla-patches-exploitable-bigsig-cryptographic-bug/

Renowned bug-hunter Tavis Ormandy of Google's Project Zero team recently found a critical security flaw in Mozilla's cryptographic code.

Many software vendors rely on third-party open source cryptographic tools, such as OpenSSL, or simply hook up with the cryptographic libraries built into the operating system itself, such as Microsoft's Secure Channel (Schannel) on Windows or Apple's Secure Transport on macOS and iOS.

But Mozilla has always used its own cryptographic library, known as NSS, short for Network Security Services, instead of relying on third-party or system-level code.

Ironically, this bug is exposed when affected applications set out to test the cryptographic veracity of digital signatures provided by the senders of content such as emails, PDF documents or web pages.

In other words, the very act of protecting you, by checking up front whether a user or website you're dealing with is an imposter…

…could, in theory, lead to you getting hacked by said user or website.

As Ormandy shows in his bug report, it's trivial to crash an application outright by exploiting this bug, and not significantly more difficult to perform what you might call a "controlled crash", which can typically be wrangled into an RCE, short for remote code execution.

The vulnerability is officially known as CVE-2021-43527, but Ormandy has jokingly dubbed it BigSig, because it involves a buffer overflow provoked by submitting a digital signature signed with a cryptographic key that is bigger than the largest key NSS is programmed to expect.

Buffer overflow

A buffer overflow is triggered when a memory area that only has space for X bytes is inadvertently stuffed with Y bytes of data, where Y > X.

Those superfluous extra (Y-X) bytes of "overflow" typically end up overwriting an adjacent block of memory that is already in use for something else, like a surfeit of ill-behaved guests at a hotel room party who end up spilling out into the corridor, barging into neighouring rooms, and generally making a nuisance of themselves.

Typically, this sort of memory corruption causes the vulnerable application to veer off course into some unchartered and unknown memory region where the operating system has no choice but to shut it down right away, causing a simple crash.

But in an RCE, the attackers orchestrate the crash in such a way as to misdirect the application into code they've supplied themselves.

An RCE is like a rogue hotel partygoer who not only barges into your room and creates a disturbance that wakes you up, but also deliberately takes advantage of your temporary confusion by stealing your laptop and your wallet under cover of pretending to apologise while you chase them out.

The bad news is that any application that uses the NSS library could be affected by this bug, including most Mozilla apps and several other popular open source programs.

Mozilla explicitly lists the following as impacted:

- Thunderbird, Mozilla's own email client.
- LibreOffice, a popular free alternative to Microsoft Office.
- Evolution, an open source calendaring app.
- Evince, a popular multi-format document viewer for PDFs and images.

The good news, if you like to think of it that way, is that this bug can't be triggered in Firefox, so Mozilla's popular browser is not affected.

Of course, there many be other apps that are vulnerable too – for example, we're not sure whether the still-active Seamonkey project, which is essentially a Firefox-like browser and a Thunderbird-like email client packaged into a single app, is at risk.

What happened?

The bug is down to code that made the infamous, and so often dangerous, assumption that "this is so unlikely that it almost certain never to happen, therefore it will never happen, therefore there is no need to check if it has".

When verifying a digital signature, NSS allocates a chunk of memory to store all the data relevant to the calculations, including the cryptographic public key required for the validation.

The space reserved for the public key is chosen by working out the size of the largest possible DSA key supported by NSS, the largest possible Elliptic Curve (EC) key supported by NSS, and the largest RSA key, and then using the largest of those values to ensure a buffer that is "always big enough".

RSA keys are notoriously much larger that those of other cryptographic algorithms (this is one reason why EC cryptography is taking over from RSA), typically reaching 2048 or even 4096 bits, instead of the 256 or 512 bits typically required for EC keys.

But RSA keys bigger than 4096 bits are astonishingly rare, not only because they would be much larger than is strictly needed to resist today's cracking tools, but also because they're much slower to create and use than smaller keys, even on fast computers.

We've never seen, or even heard of, RSA keys of 16384 bits in real-life use, given that they're typically between 500 and 1000 times slower to generate than 2048 bit keys, which are still currently considered acceptably large to resist attack.

Indeed, the public key buffer allocated for NSS signature verification is 16384 bits long, a size that ought to be more than enough for many years to come…

...and the code that copies an incoming public key into that buffer therefore assumes that no one would go to the trouble of generating a larger RSA key, so it doesn't bother checking that the key it just received actually fits.

The bug fix was to add in the size-checking code that ought to have been there all along.

What to do?

- Update NSS. Many Linux distros will have a central copy of the NSS library, but some installed apps may include and use their own versions of the library. You can search for the file `libnss3.so` to find how many NSS instances are on your computer. Windows apps that use NSS will typically include their own versions; search for `NSS3.DLL`. You need version 3.73 or later, or 3.68.1 ESR if you are using the extended support release. For advice on how to locate any NSS library files on your computer, and how to check what version you have, see below.

- Never skimp on error checking. Just because most people won't generate huge cryptographic keys doesn't mean that no one will, whether they do so by accident (which in this case would cause a Denial of Service attack by crashing your app) or by design (in order to hack into your computer on purpose).

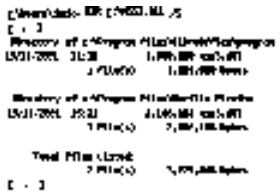
On Linux, you can search for copies of the NSS library code with the `find` command. The output from our system is shown as an example.

We have Firefox, Tor and LibreOffice installed, so we conclude from this output that Firefox and Tor have their own NSS library copies, while LibreOffice is relying on the one provided by our distro in `/usr/lib64`:

```
$ find / -type f -name 'libnss3.so' 2>/dev/null
/usr/lib64/libnss3.so
/opt/firefox/libnss3.so
/opt/tor-browser_en-US/Browser/libnss3.so
```

On Windows, try the `DIR` command shown below, from a regular command prompt window (i.e. run `CMD.EXE`, not PowerShell).

We have installed Firefox and LibreOffice, both of which contain their own copy of the NSS3 library file, and will therefore need updating via their own download sources. Remember that Firefox is not affected by this bug, but LibreOffice is.



Identifying the internal version numbers of the NSS files that turn up in tour search can be tricky, given that the only reliable way to do so is to load the library and ask it to report on itself.

51.Stanford Researchers' Quantum Computer Design Uses Single Atom to Manipulate Photons

by Matt Swayne
https://thequantuminsider.com/2021/12/02/stanford-researchers-quantum-computer-design-uses-single-atom-to-manipulate-photons/

Today's quantum computers are complicated to build, difficult to scale up, and require temperatures colder than interstellar space to operate. These challenges have led researchers to explore the possibility of building quantum computers that work using photons — particles of light. Photons can easily carry information from one place to another, and photonic quantum computers can operate at room temperature, so this approach is promising. However, although people have successfully created individual quantum "logic gates" for photons, it's challenging to construct large numbers of gates and connect them in a reliable fashion to perform complex calculations.

Now, Stanford University researchers have proposed a simpler design for photonic quantum computers using readily available components, according to a paper published Nov. 29 in Optica. Their proposed design uses a laser to manipulate a single atom that, in turn, can modify the state of the photons via a phenomenon called "quantum teleportation." The atom can be reset and reused for many quantum gates, eliminating the need to build multiple distinct physical gates, vastly reducing the complexity of building a quantum computer.

"Normally, if you wanted to build this type of quantum computer, you'd have to take potentially thousands of quantum emitters, make them all perfectly indistinguishable, and then integrate them into a giant photonic circuit," said Ben Bartlett, a PhD candidate in applied physics and lead author of the paper. "Whereas with this design, we only need a handful of relatively simple components, and the size of the machine doesn't increase with the size of the quantum program you want to run."

This remarkably simple design requires only a few pieces of equipment: a fiber optic cable, a beam splitter, a pair of optical switches and an optical cavity.

Fortunately, these components already exist and are even commercially available. They're also continually being refined since they're currently used in applications other than quantum computing. For example, telecommunications companies have been working to improve fiber optic cables and optical switches for years.

"What we are proposing here is building upon the effort and the investment that people have put in for improving these components," said Shanhui Fan, the Joseph and Hon Mai Goodman Professor of the

School of Engineering and senior author on the paper. "They are not new components specifically for quantum computation."

A novel design

The scientists' design consists of two main sections: a storage ring and a scattering unit. The storage ring, which functions similarly to memory in a regular computer, is a fiber optic loop holding multiple photons that travel around the ring. Analogous to bits that store information in a classical computer, in this system, each photon represents a quantum bit, or "qubit." The photon's direction of travel around the storage ring determines the value of the qubit, which like a bit, can be 0 or 1. Additionally, because photons can simultaneously exist in two states at once, an individual photon can flow in both directions at once, which represents a value that is a combination of 0 and 1 at the same time.

The researchers can manipulate a photon by directing it from the storage ring into the scattering unit, where it travels to a cavity containing a single atom. The photon then interacts with the atom, causing the two to become "entangled," a quantum phenomenon whereby two particles can influence one another even across great distances. Then, the photon returns to the storage ring, and a laser alters the state of the atom. Because the atom and the photon are entangled, manipulating the atom also influences the state of its paired photon.

"By measuring the state of the atom, you can teleport operations onto the photons," Bartlett said. "So we only need the one controllable atomic qubit and we can use it as a proxy to indirectly manipulate all of the other photonic qubits."

Because any quantum logic gate can be compiled into a sequence of operations performed on the atom, you can, in principle, run any quantum program of any size using only one controllable atomic qubit. To run a program, the code is translated into a sequence of operations that direct the photons into the scattering unit and manipulate the atomic qubit. Because you can control the way the atom and photons interact, the same device can run many different quantum programs.

"For many photonic quantum computers, the gates are physical structures that photons pass through, so if you want to change the program that's running, it often involves physically reconfiguring the hardware," Bartlett said. "Whereas in this case, you don't need to change the hardware – you just need to give the machine a different set of instructions."

Stanford postdoctoral scholar Avik Dutt is also co-author of this paper. Fan is a professor of electrical engineering, a member of Stanford Bio-X and an affiliate of the Precourt Institute for Energy.

This research was funded by the U.S. Department of Defense and the U.S. Air Force Office of Scientific Research.

52.How Much Has Quantum Computing Actually Advanced?

by Dan Garisto
https://spectrum.ieee.org/quantum-computing-google-sycamore

Lately, it seems as though the path to quantum computing has more milestones than there are miles. Judging by headlines, each week holds another big announcement — an advance in qubit size, or another record-breaking investment: First IBM announced a 127-qubit chip. Then QuEra announced a 256-qubit neutral atom quantum computer. There's now a new behemoth quantum computing company, "Quantinuum" thanks to the merger of Honeywell Quantum Solutions and Cambridge Quantum. And today, Google's Sycamore announced another leap toward quantum error correction.

A curmudgeon might argue that quantum computing is like fusion, or any promising tech whose real rewards are—if even achievable—decades off. The future remains distant, and all the present has for us is smoke, mirrors, and hype.

To rebut the cynic, an optimist might point to the glut of top-tier research being done in academia and industry. If there's new news each week, it's a sign that sinking hundreds of millions into a really hard problem does actually reap rewards.

For a measured perspective on how much quantum computing is actually advancing as a field, we spoke with John Martinis, a professor of physics at the University of California, Santa Barbara, and the former chief architect of Google's Sycamore.

IEEE Spectrum: So it's been about two years since you unveiled results from Sycamore. In the last few weeks, we've seen announcements of a 127-qubit chip from IBM and a 256-qubit neutral atom quantum computer from QuEra. What kind of progress would you say has actually been made?

John Martinis: Well, clearly, everyone's working hard to build a quantum computer. And it's great that there are all these systems people are working on. There's real progress. But if you go back to one of the points of the quantum supremacy experiment—and something I've been talking about for a few years now—one of the key requirements is gate errors. I think gate errors are way more important than the number of qubits at this time. It's nice to show that you can make a lot of qubits, but if you don't make them well enough, it's less clear what the advance is. In the long run, if you want to do a complex quantum computation, say with error correction, you need way below 1% gate errors. So it's great that people are building larger systems, but it would be even more important to see data on how well the qubits are working. In this regard, I am impressed with the group in China who reproduced the quantum supremacy results, where they show that they can operate their system well with low errors.

I want to drill down on "scale versus quality," because I think it's sort of easy for people to understand that 127 qubits is more qubits.

Yes, it's a good advance, but computer companies know all about systems engineering, so you have to also improve reliability by making qubits with lower errors.

So I know that Google, and I believe Chris Monroe's group, have both come up with fault tolerance results this year. Could you talk about any of those results?

I think it's good that these experiments were done. They're a real advance in the field to be able to do error correction. Unfortunately, I don't completely agree calling such experiments fault tolerance, as it makes one think like you've solved error correction, but in fact it's just the first step. In the end, you want to do error corrections so that the net logical error [rate] is something like 10^{-10} to 10^{-20}, and the experiments that were done are nowhere telling you yet that it's possible.

Yeah, I think they're like 10^{-3}.

It depends how you want to quantify it, but it's not a huge factor. It could be a bit better if you had more qubits, but you would maybe have to architect it in a different way. I don't think it is good for the field to oversell results making people think that you're almost there. It's progress, and that's great, but there still is a long way to go

I remember that IBM had, once upon a time, touted their quantum volume as a more appropriate universal benchmark. Do you have thoughts about how people can reasonably compare claims between different groups, even using different kinds of qubits?

Metrics are needed, but it is important to choose them carefully. Quantum volume is a good metric. But is it really possible to expect something as new and complex as a quantum computer system to be characterized by one metric? You know, you can't even characterize your computer, your cell phone, by one metric. In that case, if there's any metric, it's the price of the cell phone.

I think it is more realistic at this time to consider a suite of metrics, something that needs to be figured out in the next few years. At this point, building a quantum computer is a systems engineering problem, where you have to get a bunch of components all working well at the same time. Quantum volume is good because it combines several metrics together, but it is not clear they are put together in the best way. And of course if you have a single metric, you tend to optimize to that one metric, which is not necessarily solving the most important systems problems. One of the reasons we did the quantum supremacy experiment was because you had to get everything working well, at the same time, or the experiment would fail.

I mean, from my perspective, really the only thing that's been a reliable benchmark—or that I even get to see—is usually some kind of sampling problem, whether it's boson sampling or Gaussian boson sampling. As you said, it's trying to see: can you actually get a quantum advantage over these classical computers? And then, of course, you have a really interesting debate about whether you can spoof the result. But there's something happening there. It's not just PR.

Yeah. You're performing a well-defined experiment, and then you directly compare it to a classical calculation. Boson sampling was the first proposal, and then the Google theory group figured out a way to do an analogous experiment with qubits. For the boson sampling, there's a nice experiment coming from USTC in China, and there's an interesting debate that says the experiment is constructed in such a way that you can classically compute the results, whereas USTC believes there are higher-order correlations that are hard to compute. It's great the scientists are learning more about these metrics through this debate. And it's also been good that various groups have been working on the classical computation part of the Google quantum supremacy experiment. I am still interested whether IBM will actually run their algorithm on a supercomputer to see if it is a practical solution. But the most important result for the quantum supremacy experiment is that we showed there are no additional errors, fundamental or practical, when running a complex quantum computation. So this is good news for the field as we continue to build more powerful machines.

It's interesting, because I think there is that real interplay between the theory and the experiment, when you get to this cutting edge stuff, and people aren't quite sure where either side is and both keep making advances forward.

For classical computers, there has always been good interplay between theory and experiment. But because of the exponential power of a quantum computer, and because the ideas are still new and untested, we are expecting scientists to continue to be quite inventive.

What does the next step look like for quality? You were saying that that's the main roadblock. We are so far from having the kind of fidelity that we need. What is the next step for error correction? What should we be looking for?

In the last year Google had a nice paper on error correction for bit flips or phase flips. They understood the experiment well, and discussed what they would have to do for error correction to work well for having both bit and phase at the same time. It has been clear for some time that the major advance is to improve gate errors, and to build superconducting qubits with better coherence. That's also something that I've been thinking about for a couple years. I think it's definitely possible, especially with the latest IBM announcement that they were able to build their 127-qubit device with long coherence times throughout the array. So for example, if you could have this coherence in the more complex architecture of the Google Sycamore processor, you would then have really good gate errors well below 0.1%. This is of course not easy because of systems engineering issues, but it does show that there is a lot of room for improvement with superconducting qubits.

You were saying that there is a trade-off between the gate coupling control and the coherence time of the qubit. You think we can overcome that trade-off?

Obviously the engineering and the physics pushes against each other. But I think that can be overcome. I'm pretty optimistic about solving this problem. People know how to make good devices at this time, but we probably need to understand all the physics and constraints better, and to be able to predict the coherence accurately. We need more research to improve the technology readiness level of this technology.

What would you say is the most overlooked, potential barrier to overcome? I've written about control chips, the elimination of the chandelier of wires, and getting down to something that's actually going to fit inside your dil fridge.

I have thought about wiring for about five years now, starting at Google. I can't talk about it, but I think there's a very nice solution here. I think this can be built given a focussed effort.

Is there anything we haven't talked about that you think is important for people to know about the state of quantum computing?

I think it's a really exciting time to be working on quantum computing, and it's great that so many talented engineers and scientists are now in the field. In the next few years I think there will be more focus on the systems engineering aspects of building a quantum computer. As an important part of systems engineering is testing, better metrics will have to be developed. The quantum supremacy experiment was interesting as it showed that a powerful quantum computer could be built, and the next step will be to show both a powerful and useful computer. Then the field will really take off.

Some kind of standardization.

Yes, this will be an important next step. And I think such a suite of standards will help the business community and investors, as they will be better able to understand what developments are happening.

Not quite a consumer financial protection bureau, but some kind of business protection for investors.

With such a new technology, it is hard to understand how progress is being made. I think we can all work on ways to better communicate how this technology is advancing. I hope this Q&A has helped in this way.

53.A quantum of disruption

by Alan Burkitt-Gray
https://www.capacitymedia.com/articles/3830275/a-quantum-of-disruption

The way we secure our internet data is broken – or fairly close to being broken. Our curtain of confidentiality will soon be ripped away by new, powerful computing technology. Fortunately, there's other technology that's coming along that, some say, will help us protect communications even more securely than before.

Confusingly, there's a single word attached to both the new method of attack and the new method of protection: quantum. Both attack and defence are rooted in quantum physics – but, I promise, we'll leave the science alone.

Why is it important? Let's start with a question. If you have data that's stored in your systems and – because it always is these days – transmitted over fibre to other locations, how difficult for you would it be if it were released to a competitor, or a customer, or a lawyer, or a government? Not necessarily now but in, say, 2027, or 2032?

That could be your company's financial information; or the medical records you are storing for a hospital; or designs for a new system – everything from a new car to a missile. How about your customers' private data? Or your employees' private data? Your emails? Your browsing habits? You bank account information and your travel history?

Some of this might be embarrassing if it were to be released or leaked. Some might be expensive or confidence-wrecking. Some might be career-ending.

In this feature I'm writing about why public-key cryptography (PKC) is at the end of its life after a remarkable 40 years or so. Of course, the industry hasn't been using PKC for 40 years – mainly because it's only in the past 20 years that we have been buying things on the internet, and therefore have wanted to keep our account information secret as it whizzed across the network.

But the security of cryptography is about to be compromised by the arrival of new quantum-based computing techniques. At the same time new quantum-based cryptography techniques are coming, like the US Cavalry riding to the rescue of the Wells Fargo stagecoach, full of money, that's about to be attacked by bandits.

Where the data is

A dumb reporter once asked a bank robber, Willie Sutton, why he robbed banks. "Because that's where the money is," he is alleged to have said, though later in life he denied that. Not the well-protected stagecoaches, you note: the banks.

In the same way, if you want to steal someone's data, go for the nodes rather than the quantum-protected fibre links: that's where the data is, as Sutton might have said.

Some say that quantum key cryptography (QKC) is the answer. Others say QKC is already broken and will be supplanted by post-quantum algorithms (PQA). Yet others say, nope, that's no good either and here, out of the bag of tricks, is yet another quantum-related suggestion.

It's clear, though, that cryptography as it is used in data communications today is nearing the end of its life. We are either going to go back to writing things on the back of postcards or we are going to have to find a better way.

Normally when anyone decides to write about quantum science or technology, they start by talking about Albert Einstein, Erwin Schrödinger – the cat man – and Werner Heisenberg. I've done it myself. I've quoted Einstein's reputed comment that quantum science is "spooky action at a distance" and his question: "Does God play dice?"

And then we all go off to write about strangeness, and duality, and all the other things that are associated with quantummery. (I made that word up, by the way; if it's in the OED or Webster's Dictionary in 20 years, blame me.)

But I and my colleagues on Capacity, when we write about data centres, optical fibres and 5G, don't discuss how transistors work in integrated circuits, how the refractive index of glass confines light to fibre, or Maxwell's laws of electromagnetism. That's because we are not talking about how it works, but what it all means and how it affects you in the industry. And this is what I want to do about quantum technology.

All this quantum science is leading to a technology that will arrive in your networks and data centres within a few years – five, maybe, or 10 or 15. That's OK, you say. Plenty of time for the CTO to worry about it – or the CTO's successor.

Misrouted data

But your data is already being compromised. It's being misrouted over the internet, through apparently sporadic errors in border gateway protocol (BGP), the rules that allow the systems that make up the internet to send your information in the right direction.

There have been a few instances in the past few years where, for some inexplicable reason, traffic has gone off in a weird direction. It always ended up where it was supposed to be heading, but the idea is around that someone was intercepting the information, copying it and squirrelling it away, for the day when quantum computers would allow them to decode and read it.

Who says so? For a start, listen to Laura Thomas, a former CIA case officer who was the agency's chief of base in Afghanistan. (Search online for her extraordinarily moving piece in The Cipher Brief on the West's disastrous record in Afghanistan in 2020-21. Don't bother looking at LinkedIn for her career history, though: her first job listed was in March 2021.)

Thomas, who is now senior director of national security solutions at Dan Caruso's company, ColdQuanta, says these are "BGP hacks" and warns: "We know countries are harvesting data – it's called harvest now, decrypt later. There's a lot they can do. It's like gold."

Others in the industry agree. There are carriers – you've met them, I've met them – that are implicated in diverting traffic through nodes in places that are, shall we say, unfriendly to the West.

So, let's look at quantum computing, and what it promises, and what it threatens. And then go on to ways of protecting data against the new threat – new data at least.

Andersen Cheng is CEO of a small cybersecurity company called Post-Quantum. He used to be with JP Morgan and then with the Carlyle Group, the private equity investor. He got involved in crypto in 2003 when he joined TRL Technology, which sells cyber security and counter terrorism solutions to governments.

Why is current cryptography under threat, I asked him. "A classical computer does serial computations, but very fast. There are many things a quantum machine can do, but it is useless at doing that. It is extremely powerful in doing the same thing over and over, a million times – and again and again."

Prime numbers

Why is that important? At the heart of current cryptography is the multiplication of two prime numbers to produce a larger number. And then its factorisation back into the two primes.

Easy for short numbers, "but there are hundreds of numbers that it takes years to factorise," Cheng tells me. In order to encrypt your data – for a bid on eBay or a supermarket purchase, or an ordinary email – the system uses long prime numbers. Conventional computers will crunch away for years: too long to be worthwhile. What you need is an answer in minutes or seconds.

Quantum computers that will do it in a short time "are becoming more available", says Duncan Jones, head of quantum cyber security at Cambridge Quantum, a company that is in the process of merging with the quantum division of Honeywell. Cloud-based quantum computing services will be on the market in 2022, and that will mean that "people can genuinely experiment", Jones says.

Like the CIA, which ColdQuanta's Thomas used to work for, the UK's National Cyber Security Centre (NCSC) has been aware of the threat for some time. The centre updated its white paper, Preparing for Quantum-Safe Cryptography, in November 2020. The "mathematical problems [of decoding encrypted information] would be easy to solve on a large, general-purpose quantum computer", says NCSC, which is part of Government Communications Headquarters, one of the UK's three main intelligence agencies.

So be warned. Current cryptography is obsolescent, if not already obsolete. What do you do to protect future data communications against the predations of quantum computing?

Quantum hype cycle

Here, the honest answer is: We don't yet know. Or we can't yet be sure. We are in the early phase of the quantum hype cycle, and different people are proposing different possible solutions.

Quantum-safe communications relies on the transmission of individual quantums of light to carry the keys that are used to encrypt the main data traffic. And, if the stream of quantums is intercepted, the quantums don't get through – a quantum is either there or it isn't. If it isn't, you know there's a problem, you know your signal is compromised, so you ignore that bit of the message. Quantum people talk happily of sending a new encryption key via QKD every few seconds.

Andrew Lord, senior manager of optical research at BT's laboratories, and his team are working closely with Toshiba to try QKD in real-life communications. He's running two trials, including one connecting London's two main financial centres, the City, as it's called, and Canary Wharf, just to the east.

"We are asking: 'How do you use a [quantum] network? What would customers use this for?'," he says. The idea is to test how quantum-secure networks will be used in real life – and to test their weak spots. "We have three exchanges that are clustered. The customer can go into one of these exchanges and come out of another. That's harder to do in a secure way. You have to guarantee not getting keys to the wrong person."

This is being run as part of BT's regular business network, he says, installed by the company's regular technical staff. "We are selling this properly as a BT-wide trial."

No regeneration

The team has already identified some challenges – though BT is not alone in this. The biggest problem is that the quantums can't travel far down a fibre – they are, after all, individual pulses of light, and you can't even think about regenerating them, as that just replaces those quantums with others, losing the security in the process.

In June 2021, Andrew Shields, head of the quantum technology division at Toshiba Europe, reported that the company was able to transmit quantums securely as far as 600km, way more than the previous 100-200km limit.

Some are blunt to the point of cruelty. QKD is broken, they say. Even before it has started.

David Williams, founder and CEO of Arqit Quantum, wants to take it all into space. The company, having existed in stealth mode for years, did a reverse takeover by a Nasdaq-listed special-purpose vehicle, Centricus, in September 2021 that valued it at $1.4 billion. Now its market cap is $2.7 billion.

Arqit has "a lovely warm relationship with BT", which has a global deal to market its services. These will use satellites to generate and deliver true random numbers that are quantum-generated. (Among the many issues with encryption techniques is that what purport to be random numbers, essential for maximum security, aren't really random at all.)

Williams believes that not only is today's public-key cryptography broken, after it has served us for decades, but that so is the post-quantum alternative. "Eventually a clever mathematician will find how to break it," he warns.

But this is just as security is going to become rapidly more important, protecting data used for autonomous vehicles, the internet of things (IoT) and other services. "I will never put my family in an autonomous car unless it has Arqit kit," says Williams.

Satellites to data centres

He notes also that post-quantum techniques create a huge computing load, and "for small IoT sensors that simply doesn't work", says Williams. "The great thing is that all of the heavy lifting is done by these satellites sharing quantum information down to data centres."

Arqit says it has solved that problem by using its future satellites to generate truly random numbers.

So, where does this leave us? Ian West, head of the UK technology, media and telecoms practice in KPMG thinks that too many companies are leaving it too late.

"I try to explain to clients that quantum has potentially serious consequences. A really small proportion of clients are setting up quantum teams. Many are saying: 'Worry about it tomorrow.' Outside telecoms, the best I got was: 'Yes, the CTO has heard of that.' But that's not enough."

It's important that organisations set up teams of people to investigate the quantum threat and opportunities – "teams that are accountable," he says.

"And, don't make it someone's Saturday job. There is a wonderful opportunity but there is a threat as well," West adds.

The last word should go to ColdQuanta's Thomas, relatively recently out of Afghanistan.

"There is not a single bullet," she says. "Post-quantum and QKD are waypoints. As long as human beings exist there will be vulnerabilities. I'm very wary of anyone who promises a 100% secure network."

But the arrival of quantum, she says, is a technology that represents a platform shift. It's comparable with the arrival of the steam engine, electricity and the internet. "Quantum is going to be very similar, when you look back on it."

