Crypto News

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

February 1, 2021

Contents

1 IBM's top executive says, quantum computers will never reign supreme over classical ones 5

2 After SolarWinds breach, lawmakers ask NSA for help in cracking Juniper cold case 7

3 Scientists Offer Update on Desktop Quantum Computer for Education and Research 9

4 Russian Scientific Team Claims New Efficiency Record for Quantum Cryptography 10

5 Record-Breaking Source for Single Photons Developed That Can Produce Billions of Quantum Particles per Second 10

6 24 qubit GHZ entanglement at room-temperature 11

7 High-speed quantum random number generator secure against quantum attacks 12

8 How to enable quantum computing innovation through access 13

9 New "Fast Forward" Algorithm Could Unleash the Power of Quantum Computers 17

10 Iran Tests Home-Grown Quantum Cryptography On Longer Distance 18

11 KEMTLS: Cloudflare trials new encryption mechanism in anticipation of post-quantum TLS shortcomings 19

12 Long-distance and secure quantum key distribution (QKD) over a free-space channel 20

13 Certified Quantum Random Numbers from untrusted light 22

14 Cambridge quantum computing start-up targets global expansion 23

15 If You Think the Quantum Race is Only Between the U.S. and China, Think Again 24

16 The Many Ways You Can Be Phished 25

17 Cyber security – more focus required, says expert 27

18 Quantum Computer Breakthrough: New Blueprint for Better, Faster Qubit 28

19 Three Frosty Innovations for Better Quantum Computers 29

20 IBM achieves quantum computing simulation for new materials with fewer qubits 31

21 PlanQK develops AI on quantum computers 32

22 IonQ and South Korea's Q Center Announce Three-Year Quantum Alliance 33

23 Researchers improve data readout by using 'quantum entanglement' 34

24 How Quantum Computers Could Usher In a Golden Age of Computing Power 35

25 Malwarebytes breached by SolarWinds hackers 38

26 MeitY collaborates with Amazon to set up India's first quantum computing lab 39

27 The World's Top Ten Quantum Tech Universities and Research Institutions 39

28 New and Hardened Quantum Crypto System Notches "Milestone" Open-Air Test 43

29 All About Encryption Backdoors 44

30 Using drones to create local quantum networks 49

31 Intel, Cybereason Beat Ransomware With Hardware Shield 50

32 Scientists' discovery is paving the way for novel ultrafast quantum computers 52

33 Cell Phone Location Privacy 54

34 Pivotal discovery in quantum and classical information processing 54

35 Researchers conduct security analysis and improve quantum random number generation 55

36 Indian IT companies step up fight against cyberattacks 56

37 Switching to Signal? Turn on these settings now for greater privacy and security 57

38 Important Milestone in the Creation of a Quantum Computer That Uses Transistors As Qubits 58

39 Lightweight Crypto, Heavyweight Protection 60

40 Google to use quantum computing to develop new medicines 61

41 China Builds the World's First Integrated Quantum Communication Network 62

42 Electrically switchable qubit can tune between storage and fast calculation modes 63

43 Researchers realize efficient generation of high-dimensional quantum teleportation 64

44 Hackers can clone Google Titan 2FA keys using a side channel in NXP chips 65

45 Cryptography Research Centre in Abu Dhabi and Yale University to research post-quantum cryptography 67

46 Hidden Symmetry Could Be Key to Ultra-Powerful Quantum Computers 69

47 Research team demonstrates world's fastest optical neuromorphic processor 70

48 WhatsApp gives users an ultimatum: Share data with Facebook or stop using the app 71

49 Elastic Diamonds could help Quantum Computers run at room temperature 73

50 The world's first integrated quantum communication network 73

51 2021 Quantum Predictions and 2020 Predictions Analysis! 74

52 New Quantum Algorithms Finally Crack Nonlinear Equations 76

53 Robust quantum computational advantage scheme using fermion sampling 78

54 Reading out qubits like toppling dominoes: a new scalable approach towards the quantum computer 79

55 Karnataka to use blockchain for property registration **80**

56 Indian Defense Researchers Report Several Quantum Technology Advances **81**

January 2021

30 Jan 2021

1 IBM's top executive says, quantum computers will never reign supreme over classical ones

https://www.compsmag.com/news/pc/ibms-top-executive-says-quantum-computers-will-never-reign-supreme-over-classical-ones/

Processing figures quickly and on a large scale was central to computer technology. In recent decades, a new type of computing has gained a lot of interest. Quantum computers have been in development since the 1980s. They use properties of quantum physics to solve complex problems that cannot be solved with classical computers.

Companies like IBM and Google are constantly building and refining their quantum hardware. At the same time, several researchers have also explored new areas where quantum computers can cause exponential changes.

In the context of advancements in quantum technologies, The Hindu caught up with IBM Research's director Gargi Dasgupta.

Dasgupta noted that quantum computers complement traditional calculators, saying that the idea that quantum computers will take over classic computers is untrue.

"Quantum computers are not 'superior' to classical computers because of a laboratory experiment that was essentially designed [and almost certainly exclusively] implement a very specific quantum sampling procedure with no practical applications," said Dasgupta.

In order to use quantum computers on a large scale and, more importantly, to have a positive impact, it is necessary to build programmable quantum computing systems that can implement a wide variety of algorithms and programs.

Having practical applications alone will help researchers use both quantum and classical systems together for discovery in science and to create commercial value in business.

To maximize the potential of quantum computing, the industry must solve cryogenic, manufacturing and impact materials challenges at very low temperatures. This is one of the reasons IBM built its super refrigerator to house Condor, Dasgupta explained.

Quantum processors need special conditions to operate, and they need to be kept near absolute zero, like IBM's quantum chips are kept at 15 mK. The deep complexity and need for specialized cryogenics is why at least IBM's quantum computers are accessible via the cloud, and will be in the near future, noted Dasgupta, who is also IBM's CTO for the South Asia region.

Quantum computing in India

Dasgupta said interest in quantum computing in India has spiked as IBM saw a large number of exceptional participants from the country at its global and virtual events. The list included academics and professors, all of whom showed great interest in quantum computing.

In a blog published last year, IBM researchers noted that India gave quantum technology 80 billion rupees as part of its national mission for quantum technologies and applications. They believe it's a great time to get into quantum physics as the government and the people are both serious and enthusiastic about it.

Quantum computing is expanding into multiple industries, such as banking, capital markets, insurance, automotive, aerospace, and energy.

“In the coming years, the breadth and depth of the industries that use quantum will continue to grow,” noted Dasgupta.

Industries dependent on advancements in materials science will begin to explore quantum computers. Mitsubishi and ExxonMobil, for example, use quantum technology to develop more accurate chemistry simulation techniques in energy technologies.

In addition, Dasgupta said carmaker Daimler is working with IBM scientists to explore how quantum computing can be used to advance the next generation of EV batteries.

Exponential problems, such as those found in molecular simulation in chemistry, and optimization in finance, as well as machine learning, remain persistent for classical computers.

Quantum Safe Cryptography

While researchers are making progress in the field of quantum computers, some cryptocurrency enthusiasts fear that quantum computers could break security encryption. To mitigate the risks associated with cryptography services, quantum secure cryptography was introduced.

IBM, for example, offers Quantum Risk Assessment, which it claims is the world’s first quantum computing secure enterprise-class tape. It also uses Lattice-based cryptography to hide data in complex algebraic structures called lattices. Difficult math problems are useful for cryptographers, as they can use persistence to protect information and surpass the cracking techniques of quantum computers.

According to Dasgupta, even the National Institute of Standards and Technology latest list for quantum safe cryptography standards includes several candidates based on lattice cryptography.

In addition, Lattice-based cryptography is at the core of another encryption technology called Fully Homomorphic Encryption (FHE). This could make it possible to perform calculations on data without ever seeing or exposing sensitive data to hackers.

“Companies, from banks to insurers, can safely outsource the task of predicting to an untrusted environment without the risk of leaking sensitive data,” said Dasgupta.

Last year, IBM said it will unveil an 1121 qubit quantum computer by 2023. Qubit is the basic unit of a quantum computer. Prior to launch, IBM will release the 433-qubit Osprey processor. It will also release the Eagle chip with 121 qubits to reduce qubit errors and increase the number of qubits needed to achieve Quantum Advantage.

“The Condor chip with 1.121 qubits is the inflection point for low-noise qubits. By 2023, the physically smaller qubits, with on-chip isolators and signal amplifiers and multiple nodes, will be scaled to deliver Quantum Advantage’s capabilities,” said Dasgupta.

29 Jan 2021

2 After SolarWinds breach, lawmakers ask NSA for help in cracking Juniper cold case

by Sean Lyngaas

https://www.cyberscoop.com/nsa-juniper-backdoor-wyden-espionage/

As the U.S. investigation into the SolarWinds hacking campaign grinds on, lawmakers are demanding answers from the National Security Agency about another troubling supply chain breach that was disclosed five years ago.

A group of lawmakers led by Sen. Ron Wyden, D-Ore., is asking the NSA what steps it took to secure defense networks following a years-old breach of software made by Juniper Networks, a major provider of firewall devices for the federal government.

Juniper revealed its incident in December 2015, saying that hackers had slipped unauthorized code into the firm's software that could allow access to firewalls and the ability to decrypt virtual private network connections. Despite repeated inquiries from Capitol Hill– and concern in the Pentagon about the potential exposure of its contractors to the hack – there has been no public U.S. government assessment of who carried out the hack, and what data was accessed.

Lawmakers are now hoping that, by cracking open the Juniper cold case, the government can learn from that incident before another big breach of a government vendor provides attackers with a foothold into U.S. networks.

Members of Congress also are examining any role that the NSA may have unwittingly played in the Juniper incident by allegedly advocating for a weak encryption algorithm that Juniper and other firms used in its software. Lawmakers want to know if, more than a decade ago, the NSA pushed for a data protection scheme it could crack, only for another state-sponsored group to exploit that security weakness to gather data about the U.S.

"Congress has a responsibility to determine the root cause of this supply chain compromise and the NSA's role in the design and promotion of the flawed encryption algorithm that played such a central role," Wyden and other lawmakers wrote to Gen. Paul Nakasone, head of the NSA and U.S. Cyber Command, in a letter made public Friday.

Other signatories of the letter are: Sen. Cory Booker, D-N.J.; and Democratic Reps. Yvette Clarke, Anna Eshoo and Ted Lieu of California; Bill Foster of Illinois; Stephen Lynch of Massachusetts; Tom Malinowski of New Jersey; and Suzan DelBene and Pramila Jayapal of Washington.

A years-long search continues

The letter comes amid a broader search for answers in Washington as to why foreign hackers have been able to exploit the software supply chain to access sensitive government networks.

The lawmakers, for example, are asking the NSA why any security overhaul after the Juniper breach apparently did not lead the federal government to adopt defensive measures capable of detecting the SolarWinds campaign, in which suspected Russian spies infiltrated multiple federal agencies in 2020.

It's a complicated question, as there are key differences between the two incidents.

Experts regard the alleged Russian hacking spree – in which attackers breached the departments of Treasury, Justice and others – as one of the most advanced efforts in recent memory. The operation focused on multiple vendors, along with the Texas-based contractor SolarWinds, meaning that detection was no easy task.

The Juniper hack, by contrast, does not appear to have relied on so many attack vectors.

Moreover, the NSA has jurisdiction over Department of Defense networks, but not, typically, the multiple civilian agencies that have been compromised in the SolarWinds campaign. The NSA, though, is still a key player in the federal government's response to severe hacking threats.

And the parallels between the two supply chain compromises are instructive.

SolarWinds and Silicon Valley's Juniper hold similar positions in the federal contracting ecosystem. Both make software that is widely used at U.S. agencies – code that, if exploited, offers hackers a valuable entry point from which to root around in networks for sensitive data. A clear accounting of what happened in both breaches is key to improving the government's supply chain security measures, experts say.

"Whether talking about Juniper, SolarWinds or another compromise, the methods used, the weaknesses exploited and the potential scope of the ramifications need to be shared" to improve network defenses, said Ben Johnson, a former NSA official who is now chief technology officer of Obsidian Security. (Johnson left the government in 2007 and says he has no firsthand knowledge of the Juniper incident.)

A Juniper spokesperson did not respond to phone calls or emails requesting comment for this article. The NSA did not respond to a request for comment. The FBI, which Juniper has previously said was investigating the incident, did not respond to a request for comment.

Unintended consequences

Information about how still-unidentified hackers altered code on Juniper's NetScreen firmware, which runs on its firewalls, has only trickled into the public eye over the last five years.

In 2016, security researchers documented how attackers made changes to the firmware in 2012 and 2014. The 2012 change, the researchers said, was enabled by Juniper's use of a then-popular encryption algorithm known as Dual EC.

Documents leaked by former NSA contractor Edward Snowden reveal how the NSA allegedly pushed the National Institute of Standards and Technology to adopt a standard using the flawed Dual EC algorithm. The NSA reportedly knew how to break the encryption scheme to aid its overseas spying efforts.

NIST later withdrew the algorithm because of security concerns, and Juniper followed suit by removing it from its operating system in 2016. Exactly who was responsible for breaking into Juniper systems has never been publicly confirmed.

In a July 2020 letter to Wyden, Brian Martin, Juniper's general counsel, said the breach appeared to be the work of an unnamed "sophisticated nation-state hacking unit." Investigators suspected that Chinese government-backed hackers were responsible for at least one of the alterations of Juniper's code, Reuters reported in October. The attackers' tactics, techniques and procedures pointed toward Chinese-sponsored hackers, a person familiar with the investigation reiterated to CyberScoop this week.

For critics of U.S. law enforcement agencies' longstanding push for technology companies to grant access to their encrypted software products, it's a cautionary tale of unintended consequences. A foreign government had reportedly exploited a "backdoor" in encryption technology that the NSA may have helped introduce into the technology. Juniper has told congressional investigators that it added support for the Dual EC algorithm "at the request of a customer," but has refused to identify that customer, according to the lawmakers.

"What we learned here is that just a few bytes of code can be the difference between a secure system and a surveillance bonanza for our foreign adversaries," said Matthew Green, an associate professor of computer science at Johns Hopkins University and one of the authors of the 2016 research paper on the Juniper breach.

"The only solution we have to this problem is transparency, to make sure nothing like this can ever happen again," Green added.

Juniper's Martin also said in his letter to Wyden that the firm believed it had "successfully remediated the attack," while asserting that the "intrusion was neither caused nor aided by the use of" the Dual EC algorithm.

That is technically true, Green said, in that the attackers didn't break into Juniper using the Dual EC algorithm, but it obscures the broader point: The hackers apparently used their access to Juniper firmware to modify the algorithm and enable their spying.

A clear post-mortem report on the Juniper breach remains elusive. NSA officials told Wyden's office in a 2018 briefing that the agency had written a "lessons learned" report about the Dual EC incident, according to Keith Chu, a Wyden spokesman. But the NSA now asserts that it cannot locate the document, Chu said. The NSA did not respond to questions on the matter from CyberScoop.

Wyden and the other legislators asked NSA about the status of that report again on Friday.

3 Scientists Offer Update on Desktop Quantum Computer for Education and Research

by Matt Swayne

https://thequantumdaily.com/2021/01/29/scientists-offer-update-on-desktop-quantum-computer-for-education-and-research/

Scientists from quantum startup SpinQ Technology gave new details on its commercial two-qubit desktop quantum computer that can be used for educational purposes – and hinted at future directions for the machine.

The team reported on the device – originally launched in January 2020 as SpinQ Gemini – in ArXiv, a preprint research server. According to the researchers, this first-generation product is an integrated hardware-software system.

The hardware is based on a Nuclear Magnetic Resonance – or NMR – spectrometer that uses permanent magnets. The device operates under room temperature ($0 - 30°C$) and only weighs about 55 kg. The scientists say the design, which is aimed at K-12 and university-level students, works for classroom use because it is cost effective, costing about $50,000 (US), and is easy to maintain.

The NMR model is critical to make a portable, desktop quantum machine, according to the research team, adding "With the development of permanent magnet technology in recent years, it is possible to bring down the size and cost of NMR spectrometers [42-46]. This then makes theNMR technology an ideal choice for building portable quantum computers."

The quantum control capabilities help students and researchers learn about quantum control and quantum noise, the researchers report.

They added that institutions in Canada, Taiwan and Mainland China are now using the device.

The team wants to create new generations of the the SpinQ quantum computer that have more qubits and advanced control functions for researchers with comparable cost. They are also trying to significantly bring down the cost of the machine, aiming at a quantum computer that could be sold for under 5,000 USD) for K-12.

"We believe that low-cost portable quantum computer products will facilitate hands-on experience for teaching quantum computing at all levels, well-prepare younger generations of students and researchers for the future of quantum technologies," the team wrote.

28 Jan 2021

4 Russian Scientific Team Claims New Efficiency Record for Quantum Cryptography

https://quantumcomputingreport.com/russian-scientific-team-claims-new-efficiency-record-for-quantum-cryptography/

A group of scientists from the Russian Quantum Center along with others from Russian cybersecurity startup QRate have announced two achievements that they contend will contribute to setting the world record for efficiency of classical post-processing algorithms for QKD. The first is a new protocol for the information reconciliation stage of quantum key distribution based on polar codes which makes them more resistant to environmental noise. The second is a method of reducing the portion of quantum-generated secret keys, that is consumed during the authentication procedure using a lightweight authentication protocol for QKD based on a ping-pong scheme for the QKD authenticity check. The group claims that this new method reduces the portion of quantum-generated secret keys consumed for the authentication purposes to below 1%. Together, the researchers say that these two developments will help provide the record efficiencies that they claim. Both developments have been published in the IEEE Xplore data base.

5 Record-Breaking Source for Single Photons Developed That Can Produce Billions of Quantum Particles per Second

by University of Basel

https://scitechdaily.com/record-breaking-source-for-single-photons-developed-that-can-produce-billions-of-quantum-particles-per-second/

Researchers at the University of Basel and Ruhr University Bochum have developed a source of single photons that can produce billions of these quantum particles per second. With its record-breaking efficiency, the photon source represents a new and powerful building-block for quantum technologies.

Quantum cryptography promises absolutely secure communications. A key component here are strings of single photons. Information can be stored in the quantum states of these light particles and transmitted over long distances. In the future, remote quantum processors will communicate with each other via single photons. And perhaps the processor itself will use photons as quantum bits for computing.

A basic prerequisite for such applications, however, is an efficient source of single photons. A research team led by Professor Richard Warburton, Natasha Tomm and Dr. Alisa Javadi from the University of Basel, together with colleagues from Bochum, now reports in the journal Nature Nanotechnology on the development of a single-photon source that significantly surpasses previously known systems in terms of efficiency.

“Funnel” guides light particles

Each photon is created by exciting a single “artificial atom” (a quantum dot) inside a semiconductor. Usually, these photons leave the quantum dot in all possible directions and thus a large fraction is lost. In the photon source now presented, the researchers have solved this problem by positioning the quantum dot inside a “funnel” to send all photons in a specific direction.

The “funnel” is a novel micro-cavity that represents the real innovation of the research team: The micro-cavity captures almost all of the photons and then directs them into an optical fiber. The photons, each about two centimeters long, emerge at the end of an optical fiber.

The efficiency of the entire system – that is, the probability that excitation of the quantum dot actually results in a usable photon – is 57%, more than double that of previous single-photon sources. “This is a really special moment,” explains lead author Richard Warburton. “We’ve known for a year or two what’s possible in principle. Now we’ve succeeded in putting our ideas into practice.”

Enormous increase in computing power

The increase in efficiency has significant consequences, Warburton adds: “increasing the efficiency of single photon creation by a factor of two adds up to an overall improvement of a factor of one million for a string of, say, 20 photons. In the future, we’d like to make our single-photon source even better: We’d like to simplify it and pursue some of its myriad applications in quantum cryptography, quantum computing and other technologies.”

6 24 qubit GHZ entanglement at room-temperature

https://www.swissquantumhub.com/24-qubit-ghz-entanglement-at-room-temperature/

Austrian AQT startup has just announced their compact ion-trap quantum computer prototype, demonstrating 24 qubit GHZ entanglement in a room-temperature setup housed in two 19-inch racks.

This research work in cooperation with the University of Innsbruck, ETH Zürich and the Russian Quantum Center, marks an important step in the steady progress of Quantum Information Processing (QIP) from a purely academic discipline towards applications throughout science and industry.

Transitioning from lab-based, proof-of-concept experiments to robust, integrated realizations of QIP hardware is a crucial step in this process.

The team has presented a 19-inch rack quantum computing demonstrator based on $^{40}Ca^{+}$ optical qubits in a linear Paul trap to address many of these challenges.

They have outlined the mechanical, optical, and electrical subsystems and also describe the automation and remote access components of the quantum computing stack.

They have also described characterization measurements relevant to digital quantum computing including entangling operations mediated by the Molmer-Sorenson interaction.

Using this setup they have produced maximally-entangled Greenberger-Horne-Zeilinger states with up to 24 ions without the use of post-selection or error mitigation techniques.

7 High-speed quantum random number generator secure against quantum attacks

by Dino Solar Nikolic

https://www.fysik.dtu.dk/english/about-dtu-physics/news/Nyhed?id=%7BC9FFA31D-F951-436A-B782-48A3D8E41600%7D

At first glance, random numbers may seem trivial to produce and utterly useless. Not an easy sell. Isn't it just a matter of flipping a coin? Not quite!

A burning platform

Realizing that random numbers are the very backbone of encryption, cyber security, and ultimately our trust in a digitized society, immediately provides another perspective on the business case. It may also make you more anxious about when 'random' is actually random enough to keep your personal information and bank transactions secure. Not just now, but also in the future.

"Computing power keeps increasing at an exponential pace and quantum computers, capable of shattering current cryptographic schemes, are lurking around the corner. This makes generation of true and quantum-secure random numbers one of the key challenges for a future secure communication infrastructure", says Ulrik Lund Andersen, leader of the DNRF center bigQ at DTU Physics.

Some are more random than others

Randomness comes in many flavors and most random number generators (RNG) are actually predictable deep down because they rely on algorithms designed to produce randomness.

When looked at in the right way, the determinism of the algorithm will reveal itself in the numbers, disclosing a predictable pattern. For that reason, such devices are termed pseudo RNGs. In many applications they are a suitable trade-off between cost and quality.For other applications, however, they are far from sufficient. If an RNG is compromised, secret information may become public with disastrous consequences.

Extracting quantum randomness

Quantum random number generators (QRNG) are fundamentally different. They directly tap into the probabilistic nature of quantum mechanics and the randomness is routed in hardware rather than algorithms. Quantum measurements yield inherently random outcomes and there is no way, even in principle, the outcome can be predicted. In other words, it is the ultimate randomness engine.

However, noise from the measurement device overlays the pure quantum mechanical randomness and provides a peephole for hackers to gain partial, but potentially devastating, information about the sourced encryption keys. The information leakage can be estimated, and countermeasures exist for regaining security. But the efficiency depends critically on assumptions about what technological powers the hacker is in possession of.

Quantum-secure and fast

Lead by Tobias Gehring, a team of researchers from bigQ have, in collaboration with the University of Sheffield, University of York and the Danish company Cryptomathic A/S, developed a QRNG device which is secure even against attacks exploiting the full potential of future quantum technologies.

“QRNG technologies usually assume that hackers are classical adversaries, meaning that they don’t have access to quantum computers or other quantum technologies. We have now closed that security gap. Our device is simple, yet it allows this important assumption to be relaxed”, says Tobias Gehring.

Not only does the demonstrated QRNG have the highest security against quantum attacks, it also boosts a 2.9 Gbit/s rate, placing it firmly among the fastest QRNG devices to date.

High-speed random number generation is important for applications such as quantum key distribution which provides encryption keys secure against attacks making use of quantum computers. High speed is also important in the cloud where the heavy data traffic consumes cryptographic keys at a very high rate.

Aim to commercialize the technology

The ambitions of the team behind this quantum breakthrough go beyond research, and the clear goal is to commercialize the QRNG device so that customers world-wide can benefit from its high-speed and future-proof random numbers in a multitude of applications.

“We will have a prototype ready for testing with potential customers in the next couple of months. We are confident in the technology and its potential and at the moment we are searching for a cofounder bringing in commercial expertise”, says Dino Solar Nikolic, who drives the commercialization process towards forming a spin-out company.

27 Jan 2021

8 How to enable quantum computing innovation through access

by Joan A. Hoffmann

https://www.brookings.edu/techstream/how-to-enable-quantum-computing-innovation-through-access/

Two recent breakthroughs in quantum computing have generated significant excitement in the field. By using quantum computers to solve problems that classical computers could not, researchers in the United States and China have separately ushered in the era of “quantum advantage.” Yet as momentous as the demonstration of quantum advantage may be, it is the availability of more capable quantum machines that will ultimately have greater impact. Access to these machines will foster a cohort of “quantum natives” capable of solving real-world problems with quantum computers.

Both recent breakthroughs – random circuit sampling by Google in 2019 and boson sampling by the University of Science and Technology of China in 2020 – are problems useful for demonstrating quantum advantage. But they do not have real-world utility and are akin to esoteric Plinko games. Neither demonstration brings us closer to identifying any near-term application for quantum computers that will drive technology development and demonstrate impact.

Although quantum computing is in its infancy, the field is already seeing significant commercial investment. The history of classical computing suggests that if this commercial activity is to continue, it is absolutely vital to identify real-world applications for near-term quantum machines, applications with real advantage over classical approaches. Doing so requires us to make quantum computing available much more widely. Fortunately, what we are also witnessing is the emergence of quantum machines sufficiently capable of engaging a broader cohort of the public – and it is this public availability that will maximize our ability to identify truly useful applications.

State of quantum computing

Decades of relentless progress in classical computing have trained technologists to expect ever-increasing compute power. Moore's Law holds that compute power will roughly double every two years, but because of recent plateauing of pure Moore's Law scaling, many technologists are now focused on what kind of computing comes next. Will it be application-specific computing? Hybrid approaches to computing technology? Or even entirely new computing paradigms?

Many have placed bets on quantum computing as an alternative paradigm with exponential performance gains over classical computing in solving certain types of problems. The long-awaited demonstration of quantum advantage appears to validate that belief.

The idea of creating a quantum computer, operating according to the laws of quantum mechanics, was suggested by Richard Feynman and others in the early 1980s. At the time, scientists were considering how best to simulate the chemical interactions ubiquitous in natural systems. What better way to simulate and understand a system following the laws of quantum mechanics than to use a computational system governed by those same quantum mechanical laws? Interest in quantum computing exploded in the mid-1990s when Peter Shor published an algorithm using a quantum computer to factor very large numbers exponentially faster than the best-known classical algorithms. The difficulty of factoring very large numbers is the basis for many modern encryption systems, and Shor's algorithm solidified the idea that a quantum computer would have applications beyond quantum mechanical simulations.

The quantum mechanical properties of superposition and entanglement together create a computing system of unprecedented complexity and power, capable of completing certain calculations exponentially faster than classical computers. But with great power comes great vulnerability: Superposition and entanglement make quantum computers exquisitely sensitive to noise and difficult to control. Unlike classical computing, where small shifts are easily rounded back to true bit values, even small errors in a qubit value will be difficult to correct. Quantum information scientists believe that algorithms known as quantum error correction (QEC) will allow us to control errors and use quantum computers for real, useful calculations.

In the quarter century since Peter Shor's factoring algorithm was published, a handful of other quantum algorithms have emerged. These include optimization, solving linear systems of equations, and approximation methods for chemical simulation. During the same period, significant hardware research has brought us to the so-called NISQ-era, that of noisy, intermediate-scale quantum machines. These small, imperfect quantum computation devices are our first opportunity to use quantum machines and test the building blocks of quantum computation. Although interesting, NISQ machines are not the large, error-corrected machines that can execute useful optimization, factoring, or simulation. We have not yet identified applications of value for near-term NISQ machines, and many scientists argue the real purpose of NISQ computers is to learn how to build better quantum computers.

Using the quantum computers of today to learn how to build the quantum computers of tomorrow may be a satisfactory scientific answer, but it is not clear that that answer is sufficient to sustain necessary interest and investment in quantum computing to continue its advancement.

Classical computing's virtuous cycle

While the exponential growth of classical computing power is well known, perhaps less known is that the cost of producing increasingly powerful computer chips also grows exponentially. But that growing cost is underwritten by exponentially increasing revenue generated by the computing industry: Revenue generated by high-impact applications is then available to be reinvested in crucial research and development activities.

As described in the National Academies' 2019 report Quantum Computing: Progress and Prospects, the cycle of increased revenue to increased manufacturing cost to increased performance served the classical computing industry, and our society, well for more than 50 years. Within this "virtuous cycle," we see a second cycle: New computing applications drew more talent into the computing ecosystem, and these talented people created the next set of industry-driving applications.

The need for applications, the need for availability

In 2009, a group of quantum information scientists published a new quantum algorithm to solve linear systems of equations – think back to high school algebra and solving "N equations for N unknowns." The ultimate impact of this algorithm was unclear, however, because the quantum efficiency would be blunted by the need to run the algorithm many times to glean all N unknowns. It took a second group of scientists, ones intimately familiar with a particular application of calculating radar cross sections, to develop a version of the algorithm in 2013 to solve for a single, concrete value – this single value being a function of all N unknowns. By needing to calculate only one value, the quantum efficiency gains are preserved.

This is what happens when we bring more and diverse voices to both quantum information and classical computational challenges. Compared to classical computing, relatively few people are thinking about quantum computing applications, which is a natural state of affairs given that quantum computers of limited capability have only recently become available.

Quantum computers are not supercharged versions of classical computers. Rather, they manipulate information in very different ways. Exploiting the power of quantum complexity for calculations of value requires more scientists familiar with quantum information processing – people who, perhaps, also possess intimate knowledge of existing computational challenges or who have innovative insights into novel capabilities not provided by classical computers.

Identifying a full complement of real-world applications for near-term quantum computers will come only with widespread access to quantum computers. Access is necessary in order to create a cohort of practitioners with the right interests and sufficient expertise to connect quantum capabilities to relevant computational problems. Broader access also creates a larger pool of innovators thinking about quantum information. Only by creating a generation of quantum hackers and tinkerers can we reach serendipitous discoveries. We may even see practical breakthroughs well before abstract understanding, as has occurred in the field of deep learning, where the ability to exploit technology has far outpaced theoretical understanding of it.

In the summer of 2019, spurred by cloud-based public access to a subset of IBM's Quantum Experience, the Johns Hopkins Applied Physics Laboratory formed an intern cohort to join the lab's quantum information team. We playfully referred to the students as our “How to Train Your Dragon” cohort – just as the younger generations of Vikings in that film harnessed the power of dragons for good, we hoped that our students would do the same for quantum computing. Composed of undergraduates with no quantum background, the cohort was exposed to a range of mathematics and physics concepts that enabled them to perform cutting-edge research within months. Their testing and evaluation of noise mitigation protocols on real quantum processors will be featured in a forthcoming technical journal publication, constituting a novel contribution to the field of quantum information. My colleagues extended this internship program the next summer to include talented high school students and saw a similar, rapid learning process, creating a new cohort of “Quantum Natives.” With access to cloud computing resources, these young scientists were able to do meaningful, breakthrough work. Imagine the breakthroughs possible if these resources were more broadly available.

Discussions of quantum computing often focus on the exotic, nonintuitive aspects of the paradigm, but our experience introducing students to quantum machines indicates that creating the quantum generation may not be so different from creating the digital generation. Early access to computers shaped the first generation of classical computing entrepreneurs. Bill Gates spent thousands of hours programming as a teenager, developing an expertise from which sprang Microsoft. Stories of serendipitous access to novel technology are all but ubiquitous among scientists, albeit with results less dramatic than Microsoft. My own earliest exposure to a computer was in the home of a friend. His father had a TRS-80 hooked up to the television with a cassette deck as the memory. We spent hours carefully programming the machine to play blackjack – our wonder tempered only slightly by unfamiliarity with the card game itself. Others have more intense reports of spending long afternoons programming university mainframes; in the 1970s, apparently, no one locked laboratory doors to tweens.

Access to the quantum cloud

Quantum computers are highly specialized machines currently not suited for life outside research laboratories, so public access to these machines currently occurs via the cloud – online access over existing internet infrastructure. The availability of early quantum computing resources will not need to be mediated by purchase of specialized equipment, creating a real opportunity for broad-based access to rather exotic technology.

Clearly, access to cloud-based quantum computing will require digital access considered ubiquitous in modern society. But virtual schooling, driven by the COVID-19 pandemic, has laid bare socioeconomic divides in technology and internet resources – resources not nearly as universal as often imagined. Quantum computing serves as one more reminder that universal digital infrastructure is absolutely vital for the education of today, the workforce of tomorrow, and participation in the technology development of the future.

Cloud-based access to quantum computing makes it easier to bring diverse voices to quantum information development and encourages cross-pollination of scientific domains, as seen in our earlier discussion of the synergy between the quantum linear systems algorithm and challenges in calculating radar cross sections. The contrast in access to quantum computers, compared to classical ones, may even sidestep phenomena partially responsible for the gender gap in computer science.

Early computer programming was frequently dominated by women. Before the 1980s, the number of women studying computer science at universities was growing faster than the number of men. This trend reversed itself in the mid-1980s, with women’s participation falling precipitously. Scholarship has traced this inflection, counterintuitively, to the emergence of personal computers. As computer hardware became more affordable and available, it was marketed very specifically to boys, creating a large computer literacy gap between men and women when they arrived at colleges, establishing a heightened expectation for existing computer skills in even introductory computer science courses. Widespread cloud access to quantum may allow us to avoid creating a similar gendered gap in quantum computer literacy.

Achieving real-world impact

While current quantum computing machines give us the opportunity to directly explore quantum algorithms and applications, these machines have not demonstrated quantum advantage with real-world impact, and we are not confident that we have identified an application that will show true advantage in the short term. The need for continued interest and investment in quantum technology demands that we identify such applications. Broader access to quantum computing resources and, with that access, broader participation will be key to formulating quantum applications.

Current public access to certain quantum computing resources puts us in a strong initial position. The classical computing industry has long maintained a beneficent relationship with higher education, contributing resources that range from student fellowships to in-kind hardware grants to free software licenses. Commercial players in quantum computing must ensure similar avenues for access for both educational and research purposes. The National Q-12 Education Partnership, a public-private effort headed by the National Science Foundation and the White House Office for Science and Technology Policy, commits to bringing quantum education to precollege students. These sorts of initiatives will bring together industry, academia, and government to expand the quantum ecosystem, within which vibrant cycles of research and development will drive progress in quantum computing.

9 New "Fast Forward" Algorithm Could Unleash the Power of Quantum Computers

by Los Alamos National Laboratory

https://scitechdaily.com/new-fast-forward-algorithm-could-unleash-the-power-of-quantum-computers/

A new algorithm that fast forwards simulations could bring greater use ability to current and near-term quantum computers, opening the way for applications to run past strict time limits that hamper many quantum calculations.

"Quantum computers have a limited time to perform calculations before their useful quantum nature, which we call coherence, breaks down," said Andrew Sornborger of the Computer, Computational, and Statistical Sciences division at Los Alamos National Laboratory, and senior author on a paper announcing the research. "With a new algorithm we have developed and tested, we will be able to fast forward quantum simulations to solve problems that were previously out of reach."

Computers built of quantum components, known as qubits, can potentially solve extremely difficult problems that exceed the capabilities of even the most powerful modern supercomputers. Applications include faster analysis of large data sets, drug development, and unraveling the mysteries of superconductivity, to name a few of the possibilities that could lead to major technological and scientific breakthroughs in the near future.

Recent experiments have demonstrated the potential for quantum computers to solve problems in seconds that would take the best conventional computer millennia to complete. The challenge remains, however, to ensure a quantum computer can run meaningful simulations before quantum coherence breaks down.

"We use machine learning to create a quantum circuit that can approximate a large number of quantum simulation operations all at once," said Sornborger. "The result is a quantum simulator that replaces a sequence of calculations with a single, rapid operation that can complete before quantum coherence breaks down."

The **Variational Fast Forwarding** (VFF) algorithm that the Los Alamos researchers developed is a hybrid combining aspects of classical and quantum computing. Although well-established theorems exclude the potential of general fast forwarding with absolute fidelity for arbitrary quantum simulations, the researchers get around the problem by tolerating small calculation errors for intermediate times in order to provide useful, if slightly imperfect, predictions.

In principle, the approach allows scientists to quantum-mechanically simulate a system for as long as they like. Practically speaking, the errors that build up as simulation times increase limits potential calculations. Still, the algorithm allows simulations far beyond the time scales that quantum computers can achieve without the VFF algorithm.

One quirk of the process is that it takes twice as many qubits to fast forward a calculation than would make up the quantum computer being fast forwarded. In the newly published paper, for example, the research group confirmed their approach by implementing a VFF algorithm on a two qubit computer to fast forward the calculations that would be performed in a one qubit quantum simulation.

In future work, the Los Alamos researchers plan to explore the limits of the VFF algorithm by increasing the number of qubits they fast forward, and checking the extent to which they can fast forward systems. The research was published September 18, 2020 in the journal npj Quantum Information.

26 Jan 2021

10 Iran Tests Home-Grown Quantum Cryptography On Longer Distance

https://menafn.com/1101497010/Iran-Tests-Home-Grown-Quantum-Cryptography-On-Longer-Distance&source=138

Researchers at the Atomic Energy Organization of Iran (AEOI) have successfully tested a home-grown version of the quantum key distribution (QKD) technology on a relatively long distance of 1650 meters.

The test carried out on Monday at Tehran's Milad Tower saw researchers use photons to carry a message encrypted through quantum keys between parties stationed at the tower and the nearby AEOI premises.

AEOI chief Ali Akbar Salehi and Iranian deputy president for scientific affair Sorena Sattari attended the ceremony to promote the home-grown QKD.

Researchers had previously tested the technology on shorter distances of two meters and 300 meters.

The tests began in 2018 when Iran announced it will become one of the few countries in the world to develop QKD.

The technology uses quantum physics rules to distribute cryptographic keys to remote parties in order to make their communication immune to cyberattacks.

Experts believe QKD would grow in significance in the upcoming years amid increasing demand for more secure channels of communication.

AEOI's Salehi said his organization is planning to launch a fourth phase of QKD test on a 7-kilometer distance between the Milad Tower and Azadi Tower in Tehran in the near future.

Salehi said the AEOI hopes it could use the QKD for secure communication between the organization's headquarters in Tehran and a major nuclear site in Fordow in central Iran.

He said the secure channel, planned to come on line in the next one or two years, would be able to carry 90 - 100 bits per seconds of data through an optic fiber network.

The AEOI has been the target of high-profile cyberattacks in the past, including on several occasions by the Israeli regime and the US.

25 Jan 2021

11 KEMTLS: Cloudflare trials new encryption mechanism in anticipation of post-quantum TLS shortcomings

by Emma Woollacott

https://portswigger.net/daily-swig/kemtls-cloudflare-trials-new-encryption-mechanism-in-anticipation-of-post-quantum-tls-shortcomings

With quantum computing looming on the horizon, Cloudflare says it has been trialing the **KEMTLS** protocol and plans to use post-quantum cryptography for most internal services by the end of this year.

The Transport Layer Security (TLS) protocol, which currently secures most internet connections, consists of a key exchange authenticated by digital signatures used to encrypt data at transport.

But, says Cloudflare, with the advent of quantum computing, TLS in its current form will be broken. While various new post-quantum cryptography algorithms have been proposed, their parameters are too large to be used for establishing efficient connections on the web.

The National Institute of Standards and Technology (NIST) is currently evaluating potential candidates, but the agency isn't expected to make its choice until 2023.

What is KEMTLS?

KEMTLS is an alternative to the TLS 1.3 handshake that uses key encapsulation mechanisms (KEMs) instead of signatures for server authentication.

The protocol was unveiled in 2020 by Peter Schwabe of the Max Planck Institute for Security and Privacy, Germany; Douglas Stebila of the University of Waterloo, Canada; and Thom Wiggers of Radboud University, Netherlands.

"We have so far tested KEMTLS only in a lab setting," Schwabe tells The Daily Swig.

"The next step before any large-scale deployment is to run KEMTLS in a small-scale experiment on confined real-world internet infrastructure to get a better understanding of the benefits and potential problems that come with deploying it on larger scale. Such an experiment is precisely what Cloudflare's plans are about."

Efficient authentication

“Alternative authentication techniques affect performance, and drop-in replacements are not always possible,” Sofía Celi, cryptography engineer with Cloudflare, tells The Daily Swig.

“However, KEMTLS is more efficient, as less data that needs to be transmitted as part of the connection.

“This does not mean that connections that use KEMTLS will be as efficient and fast as the ones we have today when using TLS 1.3, but it will mean that they will not be catastrophically slow.”

Post-quantum vision

KEMTLS has a similar structure to TLS 1.3 and, like TLS, allows clients to send encrypted data on the third message of the handshake.

“It achieves full post-quantum security for the TLS 1.3 handshake, in the sense that it encrypts the connections and also authenticates them using post-quantum algorithms,” says Celi.

“It is worth noting that post-quantum authentication for the entire connection requires more invasive WebPKI changes.”

And, says Celi, it achieves full quantum security for the TLS 1.3 handshake as it not only encrypts and secures the connections, but also allows both client and server to be authenticated.

“This means that when using KEMTLS in a world with quantum machines, the connection will be secure and the authenticity properties of it are no worse than vanilla TLS,” she says.

Positive exchange

Cloudflare says it’s currently working to see how efficiently KEMTLS works with regular connections and is prepared to use it once quantum computers arrive.

“The fact that post-quantum signatures [are] likely to be the major contributor to increasing the volume of data exchanged means it makes sense to look for authentication mechanisms that do not rely on signatures,” Professor Alan Woodward of the University of Sussex’s Surrey Centre for Cyber Security tells The Daily Swig.

“It’s already done in some secure messaging apps with end-to-end encryption in the initial key exchange, but they’re not suitable for TLS due to assumptions about who knows about which keys.

“Whether this proves to be the right solution is very much why it’s important that organisations like Cloudflare trial it at scale, and it will at least show the viability of using TLS without signatures using alternative authentication schemes based on key exchange mechanisms.”

12 Long-distance and secure quantum key distribution (QKD) over a free-space channel

by Ingrid Fadelli

https://phys.org/news/2021-01-long-distance-quantum-key-qkd-free-space.html

Quantum key distribution (QKD) is a technique that enables secure communications between devices using a cryptographic protocol that is partly based on quantum mechanics. This communication method ultimately allows two parties to encrypt and decrypt messages they send to each other using a unique key that is unknown to other parties.

Measurement-device-independent quantum key distribution (MDI-QKD) is a unique protocol that facilitates the creation of more secure QKD networks with untrusted devices. This protocol can enable QKD-based communication over longer distances, as well as higher key production rates and more reliable network verification.

So far, MDI-QKD has only been successfully implemented using fiber optics. Implementing the protocol across free-space channels, on the other hand, has proved significantly challenging.

A research group led by Jian-Wei Pan, from the University of Science and Technology in China, has recently demonstrated long-distance and secure MDI-QKD over a free-space channel for the very first time. Their paper, published in Physical Review Letters, could pave the way to satellite-based MDI-QKD implementations.

"The final goal of QKD is to realize a global-scale quantum secure communication network," Qiang Zhang, one of the researchers who carried out the study, told Phys.org. "In order to achieve this ambitious goal, two main challenges need to be addressed. One is to reduce the gap between theory and practice of QKD, and the other one is to extend the distance of QKD. The goal of our recent work was to solve these two difficulties."

Theoretically, QKD offers greater security in communications leveraging physics laws. However, imperfections and vulnerabilities of real devices could result in deviations from the models used to carry out security analyses. The MDI-QKD protocol can help to tackle this challenge by closing all loopholes on detection at once. Moreover, it can improve the performance and security of QKD implementations on real devices, by including decoy states.

Satellite-based QKD implementations could extend the distance across which this secure communication can take place, as they would enable lower transmission losses and negligible decoherence in space. By extending MDI-QKD from fiber to free-space channels, the work by Pan and his colleagues could be a first step toward implementing MDI-QKD protocols on a large scale using satellites.

"Although several fiber-based MDI-QKD experiments have been performed before our study, none of them have demonstrated the feasibility of the protocol with a free-space channel," Zhang said. "The main reason is that the amplitude and phase fluctuation induced by atmospheric turbulence makes it difficult to maintain the indistinguishability in terms of spatial, timing and spectral modes between independent photons."

As atmospheric turbulence typically destroys the spatial mode between independent photons, MDI-QKD implementations typically require the use of single-mode fiber to perform spatial filtering before applying interferometry techniques. Using single-mode fiber to couple photons, however, generally leads to a low coupling efficiency and intensity fluctuation. To solve this problem, the researchers developed a new adaptive optics system that improves the channel's overall efficiency.

"As the rapid fluctuation of light intensity makes sharing the time-frequency reference difficult, we developed new technologies to achieve high-precision time synchronization and frequency locking between independent photon sources located far apart in order to maintain the indistinguishability of the timing and spectral modes," Zhang explained. "Thanks to these technical breakthroughs, we completed a task that seemed impossible to complete before."

The study is an important milestone in the path toward implementing QKD on a large scale and using it to secure communications over longer distances. Moreover, the researchers were the first to realize photon interference in long-distance atmospheric channels. This could open up exciting possibilities for the development of complex types of quantum information processing involving quantum interference, such as quantum entanglement swapping and quantum teleportation. It could also offer new ways of testing the interface of quantum mechanics and gravity.

The researchers' long-term goal is to demonstrate satellite-based MDI-QKD and eventually to build a global quantum network. To achieve this, however, they will first need to overcome a number of additional challenges.

"One of these challenges is the high loss mainly induced by the atmospheric fluctuation," Zhang explained. "In the most straightforward configuration of satellite-based MDI-QKD, a satellite plays the role of the detection terminal (i.e., two ground stations send photons via the 'up-link' to the satellite). The channel loss measured by the Micius satellite is about 41 - 52 dB from a ground station with altitude of 5,100 miles. The loss is likely to be much higher from ground stations at a lower altitude. The single mode fiber coupling efficiency is another source of loss, which is also very significant with existing MDI-QKD systems."

In order to enable effective satellite-based MDI-QKD implementations, therefore, the researchers will first need to advance existing methods to transit photons across free-space channels. To do this, they have so far developed an adaptive optics system and an algorithm that increases the efficiency of free-space channels. In their next studies, they plan to create other algorithms and techniques for improving the overall transmission channel.

"The second challenge we hope to overcome is associated with the motion of satellites," Zhang added. "Since the signal pulses are expected to be overlapped in the time domain at the detection terminal, a very accurate prediction of a satellite's orbit is required, and the emission time of each encoded pulse should also be accurately timed, so that they can finally overlap well in the detection terminal. The Doppler frequency shift, on the other hand, is an important source of frequency mismatch that is annoying for HOM interference. The frequency of each encoded pulse should also be accurately shifted for compensation. After solving all of these technical challenges, we believe that we will be able to realize satellite-based MDI-QKD."

13 Certified Quantum Random Numbers from untrusted light

https://www.swissquantumhub.com/certified-quantum-random-numbers-from-untrusted-light/

A team of researchers from Germany, Russia and UK has designed and experimentally demonstrated an ultrafast optical Quantum Random Number Generator (QRNG) that uses a totally untrusted photonic source.

While considering completely general quantum attacks, they certified and generated in real time random numbers at a rate of 8.05 Gb/s with a composable security parameter of 10^{-10}.

Composable security is the most stringent and useful security paradigm because any given protocol remains secure even if arbitrarily combined with other instances of the same, or other, protocols, thereby allowing the generated randomness to be utilized for arbitrary applications in cryptography and beyond.

This work achieves the fastest generation of composably secure quantum random numbers ever reported.

24 Jan 2021

14 Cambridge quantum computing start-up targets global expansion

https://www.compsmag.com/news/pc/cambridge-quantum-computing-start-up-targets-global-expansion/

Riverlane is at the forefront of British start-ups seeking to be at the forefront of the most advanced technology. It develops software to help people use these advanced computers for practical purposes, increasing the chances of converting the experimental technology into commercial products.

The start-up is backed by Amadeus Capital, Arm's co-founder Hermann Hauser. On Monday, it announced its first major fundraiser, raising $ 20 million from existing owners, including the University of Cambridge and Draper Esprit, the publicly traded venture capital investment firm.

Quantum computers offer more power and can perform complex calculations to drive innovation in chemicals, pharmaceuticals and healthcare. They can also support other technologies such as machine learning and artificial intelligence.

The UK government wants to promote a world-leading quantum computing sector as part of its ambitions to put the UK at the forefront of fast-growing technology.

Last year, the Prime Minister pointed to quantum computing as one of the key areas in which the UK "leads the world" as part of his drive to make the UK a "scientific superpower". The UK is also building a national quantum computing center.

Riverlane has developed a universal operating system that enables the commercialization of quantum computers, called Deltaflow. OS – basically a system of applications that allow people to use the hugely complicated quantum hardware more easily. The quantum computers from Google and IBM run on custom operating systems.

Steve Brierley, founder of Riverlane, said, "In order for a quantum ecosystem to thrive, we urgently need an operating system. An operating system makes quantum computers useful – it allows programs and applications to run on many different machines."

Mr Brierley said the UK is already leading other countries in quantum computer hardware development, with eight of the world's 33 manufacturers within three miles of England.

"That gives us a huge advantage. We couldn't have done what we do outside the UK. It's like the early days of digital computing. We want to make it more user-friendly. "

The company expects its software to help adapt quantum computers for complicated computing work in drug discovery and materials design.

Stuart Chapman, director at Draper Esprit, who also led early investments in Graphcore, the Bristol-based AI chipmaker, said, "The next phase is where quantum computers go commercial. It's the transfer of pure science to how it rolls out. "

In the past year, Riverlane has signed up one fifth of the world's quantum hardware manufacturers to use its Deltaflow software and will use the money to expand outside the UK.

23 Jan 2021

15 If You Think the Quantum Race is Only Between the U.S. and China, Think Again

https://quantumcomputingreport.com/if-you-think-the-quantum-race-is-only-between-the-u-s-and-china-think-again/

There have recently been a number articles in the mainstream press that would lead one to the conclusion that the quantum race is limited to the U.S. versus China. These articles are ignoring that tremendous impact that Europe will have in the development and implementation of quantum technologies.

To start, let's look at some budgets. While the U.S. National Quantum Initiative Act is providing funding of $1.2 billion over a five year period, funding for quantum research in the U.S. from the private sector is at least as large as the government investment and significantly greater than any other country. The private sector funding includes venture capital investments in U.S. companies as well as corporate funding from large companies including IBM, Microsoft, Google and others. So although the private sector amounts are not made public, our estimate is that total funding including both government and private sector is in the $2 - $4 billion range over a 5 year period.

Although the China quantum investment of $10 billion has been widely reported, this figure has never been officially confirmed nor has any breakdown been released on how this money will be spent. The money will not all be spent on quantum technology R&D. It is our belief that a significant amount of China's quantum investments will be devoted to infrastructure. Some of the money will be devoted toward building a brand new Quantum Information Science Center in Hefei and additional money will be devoted towards building out China's quantum communications network. We also think that the mixture of China's quantum investments may be more heavily weighted towards quantum communications over quantum computing.

Meanwhile, multiple countries in Europe, as well as the European Commission, are making heavy quantum investments. The European Commission has allocated about $1.1 billion for its Quantum Flagship program. In addition, the individual European countries have created additional budgets to support quantum research including the UK at $1.3 billion, France at $2.2 billion, Germany at $3.1 billion, the Netherlands at $177 million, and smaller amounts in Italy, Spain, Finland, Austria and Switzerland. Although the European private sector investments are not as significant as those in the U.S., it is still present. So if you look at total European investments in quantum technologies, it will exceed $8 billion over a five year period.

But looking at raw investment numbers provides an incomplete picture, particularly when there aren't many details on how it is broken out. To look at another metric, one can look at the Top 500 listing of high performance classical computers to see where they are located. It is likely that users who are familiar with high performance computing, will also be early adopters of quantum computing. In this list, it shows that of the 500 HPC systems, the number of computers in each areas show 214 in China, 113 in the U.S., and 97 in Europe. And if you rank the Top 500 computers by performance share, the numbers show 27.5% of the total gigaflops are in the U.S., 23.3% in China and 18.3% in Europe.

One of the things that will help U.S. companies as they compete for quantum computing market share is the U.S. strength in cloud computing. Not only will the majority of quantum computing processing be delivered via the cloud, but it is likely that those enterprises that were some of earliest users of cloud technology will also be early users of quantum computing. The companies that dominate providing cloud services in the U.S. include Amazon AWS, Microsoft Azure, Google and IBM. And many European enterprises also take advantage of cloud services provided by these U.S. headquartered company. In China, the dominant cloud services provider is Alibaba.

Nonetheless, we expect that Europe will be a large player in quantum computing. In reading through several of the quantum computing national plans they imply goals of obtaining a much larger market share in quantum computing than these countries previously had achieved in classical computing. It will be interesting to see how this turns out and one should not gloss over what is happening in quantum Europe. Because in the end, it could turn out that Europe might eventually surpass the U.S., China, or both countries in the race to be the leader in quantum computing.

22 Jan 2021

16 The Many Ways You Can Be Phished

by Roger Grimes

https://blog.knowbe4.com/the-many-ways-you-can-be-phished

Social engineering and deception are as old as humanity itself. Phishing is social engineering and deception via digital means and has been with us since the beginning of computers. After early computer worms, among the very first computer crimes were fake email messages asking the recipients to do some action that was against their own best interests.

I clearly remember my experience with an ANSI bomb back in the early 1980s. An email arrived to me on a FIDOnet (an early precursor of the Internet) chat channel asking me to open and read a text file to learn how to get a free HST modem. At the time, HST modems offered 9600 baud speed, which was high tech and blazing for the time. I opened the text file with a text editor (called edlin in MS-DOS). The document contained a single, short, sentence, “Steal one!”

It was a strange line to read. I closed the document as I shook my head. Then the next key I hit formatted my hard drive! It was a tough lesson to learn. Turns out that even the simplest of documents could contain embedded, invisible printer control characters (e.g., ˆG01h), that when appropriately combined could re-map a computer keyboard so that any key hit would the perform a set of instructions. In this case, those instructions told my computer to reformat my hard drive. I’ve been distrustful of emails asking me to open documents ever since.

Since then, many more digital avenues have been developed for people to be phished and socially engineered. Social engineering and phishing are now responsible for 70% to 90% of all successful cybersecurity incidents. Here are all of the phishing methods I can think of.

Email

Email is by far the most common media channel for social engineering people. I think we are all quite acquainted with this phishing method. Phishing emails are either attempting to trick us into providing our login credentials or into opening a maliciously-rigged document or into running a Trojan Horse program. The emails will often arrive pretending to be from a person or organization that the recipient is inclined to trust.

Websites

The second most common phishing method involves websites, either using email to redirect a recipient to a malicious website or a bogus website or malicious script hosted on a legitimate website that a visitor arrives at even without an email involved. Oftentimes, completely legitimate, long-time trusted, and otherwise innocent websites are manipulated into hosting malicious content. The most common method is a malicious banner ad. The host website has allowed banner ads to be displayed while expecting only legitimate ads to be displayed, but the attacker used a variety of methods to insert their malicious script in with the legitimate ads. Or other times, the attacker simply finds and takes advantage of a vulnerability in the website to post his/her malicious script. Either way, websites are often involved in today's phishing attempts.

Social Media

Much of the world spends the majority of their time on social media sites: Facebook, Twitter, LinkedIn, Instagram, etc. So, it's no great surprise that phishers love using people's enjoyment of such sites against them. Many times, a person's legitimate social media account will be taken over by a phisher, usually from a prior involved phishing attack that tricked the legitimate owner out of their login credentials, and then that account will be used to trick others who trust the original victim.

Sadly, it can be very difficult to impossible for the original victim to reclaim control over their own social media account. Victims often lose all the content and photos they have entrusted to the social media site, losing information and memories forever. Even the social media company's proactive security measures, such as using multi-factor authentication (MFA) to protect someone's account access, can be used against the victim. I've been contacted by many dozens of people who didn't use MFA, who had their social media account taken by a phisher, and then that phisher enabled MFA, and that MFA protection prevented the original victim from ever reclaiming his/her account and content.

Browser/Desktop/Mobile Notification

A relative newcomer on the scene is that of malicious browser and desktop notifications. When a user visits a new website or application, that site or application can ask the user for permission to send him/her desktop notifications. Once approved, these notifications can be sent outside the application or website that asked for approval to send. The notifications can contain text, icons, images, multimedia content, and URLs. And like banner ads, notifications can be "rented" to others which are then involved with sending malicious or unwanted content to unsuspecting users. Because notifications are a relatively new method of transmitting malicious content, most antivirus programs do not do a good job in detecting or preventing involved malicious content.

Voice Phone Call

Phishing and social engineering can certainly come from voice calls and voicemail messages. Like all social engineering and phishing, voice-based phishing comes from someone pretending to be an otherwise trustworthy source. The originating phone number can be spoofed and the phisher or call center is often located in a foreign country, making prosecution extremely difficult. The most common voice phishing methods include fake technical support calls pretending to be from Microsoft trying to help the victim with a computer malware program and calls for victims to pay emergency fines to the IRS and law enforcement. If someone requesting an emergency payment says it's okay to pay in prepaid cards you can buy at Walmart, it's probably a request you should verify first. The big telephone companies are trying to enact new technology that prevents call number spoofing, but the defenses seem inadequate and decades too late.

Messaging/SMS

Like voice-based phishing, spoofing using short message service (SMS) texting and other messaging protocols (like Instant Rely Chat, etc.), are subject to easy origination spoofing. SMS messages can be sent by anyone and pretend to be from any phone number the spoofer wants to use. SMS messages can even appear from "short numbers" that are not phone numbers at all. Even if the phone number is real, a potential victim has no way to know if the originating phone number is valid and if who is using it is really the person or organization they say they are.

For all purposes, any phone-based media channel should be treated as untrusted by default and subject to easy spoofing. Never start performing actions that could negatively impact you without first verifying that the caller or sender is really who they say they are. It can be difficult to do that, but at the very least, the caller or sender should be able to provide a method where you can call a known, legitimate number to reach them, instead of simply relying on their inbound call or text. Sadly, at times, even legitimate services and requests cannot provide that sort of reassurance. We all await the time when phone calls and SMS messages are significantly harder to spoof.

Hybrid Combinations

It is also not rare for a phisher to use a combination of methods to win the trust of potential victims. Oftentimes, the phisher will pretext the victim by first calling or emailing a friendly, not overly suspicious message, to start establishing premature trust. Instead of asking for an action that can potentially harm the victim right away, they say hello, mention names or departments the victim is already familiar with, and so on, in order to get the victim accustomed to the new person's name and purported role. Then after the previous trust is established, the phisher will call/text/email back with the real intended request, that when executed, can harm the victim or his/her organization.

Social engineering and phishing can be done using a variety of methods. Email and websites are the most popular methods, but the other methods are becoming more and more common. As a computer security professional with 34 years of experience, any time I see a new technology, the first thing I wonder is how it can be abused by hackers and social engineers. Because if history is any guide, if a technology can be used maliciously, it will be.

It is up to us to educate others about all the ways they can be socially engineered and phished. Email and websites are just two ways. There are others. So, make sure all the people you care about and manage are aware of all the ways they can be phished. KnowBe4's technology allows you to give training and do simulated phishing across all of these methods.

17 Cyber security – more focus required, says expert

by Paul Bartlett

https://www.seatrade-maritime.com/technology/cyber-security-more-focus-required-says-expert

This was the stark message from Ben Densham, chief technology officer of Nettitude, a cyber security company owned by Lloyd's Register, as he addressed a Maritime Autonomous Systems Regulatory Conference, held virtually this week.

The incidence of attacks has increased markedly since the onset of the pandemic, he said, revealing that "the bad guys have used it to infiltrate systems". But shipping's vulnerability has never been greater, he pointed out, as the industry's digital transformation continues to accelerate. "Moving online opens up the attack surface," Densham warned, "with more opportunities for hackers."

He drew attention to the seven-month-old cyber espionage campaign, **SolarWind**, widely thought to be state-sponsored which is estimated to have infiltrated more than 18,000 targets with malicious code which initially lay dormant for some weeks. Many Fortune 500 companies are thought to have been attacked, as well as US Government departments and Microsoft.

Against a backdrop of heightened risk, Densham said that shipping needs to change its thinking. "We need to think security, not just compliance," he declared, pointing out that building cyber security into assets at the design stage is fine, but systems subsequently need constant attention in operation to guard against the speed and agility of threats and attacks in the cyber arena.

Densham stressed the importance of continuous testing of cyber resilience. As remote connectivity and varying degrees of autonomy transform many long-established shipping business models, companies must focus on cyber risks and their possible impact, he said, because they pose a constant threat that runs through all aspects of business.

In addition to its involvement in shipping and energy, Nettitude provides cyber security services to governments, the defence sector, financial services, healthcare, manufacturing and retail.

18 Quantum Computer Breakthrough: New Blueprint for Better, Faster Qubit

by Paul Scherrer Institute

https://scitechdaily.com/quantum-computer-breakthrough-new-blueprint-for-better-faster-qubits/

Researchers at the Paul Scherrer Institute PSI have put forward a detailed plan of how faster and better defined quantum bits – qubits – can be created. The central elements are magnetic atoms from the class of so-called rare-earth metals, which would be selectively implanted into the crystal lattice of a material. Each of these atoms represents one qubit. The researchers have demonstrated how these qubits can be activated, entangled, used as memory bits, and read out. They have now published their design concept and supporting calculations in the journal PRX Quantum.

On the way to quantum computers, an initial requirement is to create so-called quantum bits or "qubits": memory bits that can, unlike classical bits, take on not only the binary values of zero and one, but also any arbitrary combination of these states. "With this, an entirely new kind of computation and data processing becomes possible, which for specific applications means an enormous acceleration of computing power," explains PSI researcher Manuel Grimm, first author of a new paper on the topic of qubits.

The authors describe how logical bits and basic computer operations on them can be realized in a magnetic solid: qubits would reside on individual atoms from the class of rare-earth elements, built into the crystal lattice of a host material. On the basis of quantum physics, the authors calculate that the nuclear spin of the rare-earth atoms would be suitable for use as an information carrier, that is, a qubit. They further propose that targeted laser pulses could momentarily transfer the information to the atom's electrons and thus activate the qubits, whereby their information becomes visible to surrounding atoms. Two such activated qubits communicate with each other and thus can be "entangled." Entanglement is a special property of quantum systems of multiple particles or qubits that is essential for quantum computers: The result of measuring one qubit directly depends on the measurement results of other qubits, and vice versa.

Faster means less error-prone

The researchers demonstrate how these qubits can be used to produce logic gates, most notably the "controlled NOT gate" (CNOT gate). Logic gates are the basic building blocks that also classical computers use to perform calculations. If sufficiently many such CNOT gates as well as single-qubit gates are combined, every conceivable computational operation becomes possible. They thus form the basis for quantum computers.

This paper is not the first to propose quantum-based logic gates. "Our method of activating and entangling the qubits, however, has a decisive advantage over previous comparable proposals: It is at least ten times faster," says Grimm. The advantage, though, is not only the speed with which a quantum computer based on this concept could calculate; above all, it addresses the system's susceptibility to errors. "Qubits are not very stable. If the entanglement processes are too slow, there is a greater probability that some of the qubits will lose their information in the meantime," Grimm explains. Ultimately, what the PSI researchers have discovered is a way of making this type of quantum computer not only at least ten times as fast as comparable systems, but also less error-prone by the same factor.

19 Three Frosty Innovations for Better Quantum Computers

by Rahul Rao

https://spectrum.ieee.org/tech-talk/computing/hardware/three-super-cold-devices-quantum-computers

For most quantum computers, heat is the enemy. Heat creates error in the qubits that make a quantum computer tick, scuttling the operations the computer is carrying out. So quantum computers need to be kept very cold, just a tad above absolute zero.

"But to operate a computer, you need some interface with the non-quantum world," says Jan Cranickx, a research scientist at imec. Today, that means a lot of bulky backend electronics that sit at room temperature. To make better quantum computers, scientists and engineers are looking to bring more of those electronics into the dilution refrigerator that houses the qubits themselves.

At December's IEEE International Electron Devices Meeting (IEDM), researchers from than a half dozen companies and universities presented new ways to run circuits at cryogenic temperatures. Here are three such efforts:

- **Google's cryogenic control circuit could start shrinking quantum computers**

  At Google, researchers have developed a cryogenic integrated circuit for controlling the qubits, connecting them with other electronics. The Google team actually first unveiled their work back in 2019, but they're continuing to scale up the technology, with an eye for building larger quantum computers.

This cryo-CMOS circuit isn't much different from its room-temperature counterparts, says Joseph Bardin, a research scientist with Google Quantum AI and a professor at the University of Massachusetts, Amherst. But designing it isn't so straightforward. Existing simulations and models of components aren't tailored for cryogenic operation. Much of the researchers' challenge comes in adapting those models for cold temperatures.

Google's device operates at 4 kelvins inside the refrigerator, just slightly warmer than the qubits that are about 50 centimeters away. That could drastically shrink what are now room-sized racks of electronics. Bardin claims that their cryo-IC approach "could also eventually bring the cost of the control electronics way down." Efficiently controlling quantum computers, he says, is crucial as they reach 100 qubits or more.

- **Cryogenic low-noise amplifiers make reading qubits easier**

  A key part of a quantum computer are the electronics to read out the qubits. On their own, those qubits emit weak RF signals. Enter the low-noise amplifier (LNA), which can boost those signals and make the qubits far easier to read. It's not just quantum computers that benefit from cryogenic LNAs; radio telescopes and deep-space communications networks use them, too.

  Researchers at Chalmers University of Technology in Gothenburg, Sweden, are among those trying to make cryo-LNAs. Their circuit uses high-electron-mobility transistors (HEMTs), which are especially useful for rapidly switching and amplifying current. The Chalmers researchers use transistors made from indium phosphide (InP), a familiar material for LNAs, though gallium arsenide is more common commercially. Jan Grahn, a professor at Chalmers University of Technology, states that InP HEMTs are ideal for the deep freeze, because the material does an even better job of conducting electrons at low temperatures than at room temperature.

  Researchers have tinkered with InP HEMTs in LNAs for some time, but the Chalmers group are pushing their circuits to run at lower temperatures and to use less power than ever. Their devices operate as low as 4 kelvins, a temperature which makes them at home in the upper reaches of a quantum computer's dilution refrigerator.

- **imec researchers are pruning those cables**

  Any image of a quantum computer is dominated by the byzantine cabling. Those cables connect the qubits to their control electronics, reading out of the states of the qubits and feeding back inputs. Some of those cables can be weeded out by an RF multiplexer (RF MUX), a circuit which can control the signals to and from multiple qubits. And researchers at imec have developed an RF MUX that can join the qubits in the fridge.

  Unlike many experimental cryogenic circuits, which work at 4 kelvins, imec's RF MUX can operate down to millikelvins. Jan Cranickx says that getting an RF MUX to work that temperature meant entering a world where the researchers and device physicists had no models to work from. He describes fabricating the device as a process of "trial and error," of cooling components down to millikelvins and seeing how well they still work. "It's totally unknown territory," he says. "Nobody's ever done that."

  This circuit sits right next to the qubits, deep in the cold heart of the dilution refrigerator. Further up and away, researchers can connect other devices, such as LNAs, and other control circuits. This setup could make it less necessary for each individual qubit to have its own complex readout circuit, and make it much easier to build complex quantum computers with much larger numbers of qubits – perhaps even thousands.

21 Jan 2021

20 IBM achieves quantum computing simulation for new materials with fewer qubits

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/less-is-more-ibm-achieves-quantum-computing-simulation-for-new-materials-with-fewer-qubits/

While the scientific community holds its breath for a large-scale quantum computer that could carry out useful calculations, a team of IBM researchers has approached the problem with an entirely different vision: to achieve more and better results right now, even with the limited quantum resources that exist today.

By tweaking their method, the scientists successfully simulated some molecules with a higher degree of accuracy than before, with no need for more qubits. The researchers effectively managed to pack more information into the mathematical functions that were used to carry out the simulation, meaning that the outcome of the process was far more precise, and yet came at no extra computational cost.

“We demonstrate that the properties for paradigmatic molecules such as hydrogen fluoride (HF) can be calculated with a higher degree of accuracy on today’s small quantum computers,” said the researchers, at the same time priding themselves on helping quantum computers “punch above their weight”.

Car manufacturer Daimler, a long-term quantum research partner of IBM’s, has shown a strong interest in the results, which could go a long way in developing higher-performing, longer-lasting and less expensive batteries.

Since 2015, Daimler has been working on upgrading lithium-ion batteries to lithium-sulfur ones – a non-toxic and easily available material that would increase the capacity and speed-of-charging of electric vehicles.

Designing a battery based on new materials requires an exact understanding of which compounds should come together and how. The process involves accurately describing all the characteristics of all the molecules that make up the compound, as well as the particles that make up these molecules, to simulate how the compound will react in many different environments. In other words, it is an incredibly data-heavy job, with infinite molecular combinations to test before the right one is found.

The classical methods that exist today fail to render these simulations with the precision that is required for a breakthrough such as the one Daimler is working towards. “This is a big problem to develop next-generation batteries,” Heike Riel, IBM Research quantum lead, told ZDNet. “Classical computers, and the models we’ve developed in physics and chemistry for many years still cannot solve those problems.”

But the task could be performed at speed by quantum computers. Qubits, and their ability to encode different information at the same time, enable quantum algorithms to run several calculations at once – and are expected, one day, to enable quantum computers to tackle problems that are seemingly impossible, in a matter of minutes.

To do that, physicists need quantum computers that support many qubits; but scaling qubits is no piece of cake. Most quantum computers, including IBM's, work with less than 100 qubits, which is nowhere near enough to simulate the complex molecules that are needed for breakthroughs, such as lithium-sulfur car batteries.

Some of the properties of these molecules are typically represented in computer experiments with a mathematical function called a Hamiltonian, which represents particles' spatial functions, also called orbitals. In other words, the larger the molecule, the larger the orbital, and the more qubits and quantum operations will be needed.

"We currently can't represent enough orbitals in our simulations on quantum hardware to correlate the electrons found in complex molecules in the real world," said IBM's team.

Instead of waiting for a larger quantum computer that could take in weighty calculations, the researchers decided to see what they could do with the technology as it stands. To compensate for resource limitations, the team created a so-called "transcorrelated" Hamiltonian – one that was transformed to contain additional information about the behavior of electrons in a particular molecule.

This information, which concerns the propensity of negatively charged electrons to repel each other, cannot usually fit on existing quantum computers, because it requires too much extra computation. By incorporating the behavior of electrons directly into a Hamiltonian, the researchers, therefore, increased the accuracy of the simulation, yet didn't create the need for more qubits.

The method is a new step towards calculating materials' properties with accuracy on a quantum computer, despite the limited resources available to date. "The more orbitals you can simulate, the closer you can get to reproducing the results of an actual experiment," said the scientists. "Better modelling and simulations will ultimately result in the prediction of new materials with specific properties of interest."

IBM's findings might accelerate the timeline of events for quantum applications, therefore, with new use cases emerging even while quantum computers work with few qubits. According to the researchers, companies like Daimler are already keen to find out more about the breakthrough.

This is unlikely to shift IBM's focus on expanding the scale of its quantum computer. The company recently unveiled a roadmap to a million-qubit system, and said that it expects a fault-tolerant quantum computer to be an achievable goal for the next ten years. According to Riel, quantum simulation is likely to be one of the first applications of the technology to witness real-world impacts.

"The car batteries are a good example of this," she said. "Soon, the number of qubits will be enough to generate valuable insights with which you can develop new materials. We'll see quantum advantage soon in the area of quantum simulation and new materials."

IBM's roadmap announces that the company will reach 1,000 qubits in 2023, which could mark the start of early value creation in pharmaceuticals and chemicals, thanks to the simulation of small molecules.

21 PlanQK develops AI on quantum computers

by Nick Flaherty

https://www.eenewseurope.com/news/planqk-quantum-ai-computers

A major project in Germany is using quantum computing techniques to develop quantum AI algorithms.

The €19m **PlanQK** project (**Platform and Ecosystem for Quantum-Assisted Artificial**

Intelligence) is funded by the German Federal Ministry of the Economy and now has 15 partners and 33 associated partners, including Siemens and Daimler.

The latest member, Deutsche Telekom (DT), is researching and testing potential use cases from the perspective of a network operator. This includes network security as well as data routing algorithms.

Quantum computers promise an exponential increase in processing speed for selected problem classes. For example, in combinatorial optimization problems or the training of AI models. In communication science, Shor's algorithm is usually considered the "killer application" of quantum computing as the systems can use it to attack today's security infrastructures.

In the PlanQK project, DT's Telekom Innovation Labs (T-Labs) provides some specific use cases from the field of telecommunications. These include the optimization of communication networks, Industry 4.0 applications or AI-clustering problems for particular applications.

These applications have a high level of complexity and, if the problem exceeds a critical size, can only be calculated classically with great difficulty. Here, quantum algorithms promise the solution. With growing size, quality and processing speed, quantum computers could find their way into Telekom's operational business.

The project is developing a vendor-independent platform and associated ecosystem for quantum AI. Users could then, for example, compile solutions for their company or commission them via the cloud or a quantum app store.

PlanQK follows a completely different path to the software development kits provided by quantum computer developers, as it is not a development environment for quantum software and is intended to be absolutely SDK neutral. The software provided in PlanQK can be created with any such SDK by using the concept of patterns, proven solutions to recurring problems in quantum computing. By definition, the solutions provided in such patterns are implementation- and vendor-neutral. A pattern then refers to possibly different quantum AI implementations created by "any" quantum SDK.

22 IonQ and South Korea's Q Center Announce Three-Year Quantum Alliance

by Matt Swayne

https://thequantumdaily.com/2021/01/21/ionq-and-south-koreas-q-center-announce-three-year-quantum-alliance/

IonQ, a leader in quantum computing, announced a three-year alliance with South Korea's Quantum Information Research Support Center, or Q Center, according to a news release. The Q Center is an independent organization at Sungkyunkwan University (SKKU) focused on the creation of a rich research ecosystem in the field of quantum information science. The partnership will make IonQ's trapped-ion quantum computers available for research and teaching across South Korea.

IonQ's systems have the potential to solve the world's most complex problems with the greatest accuracy. To date, the company's quantum computers have a proven track record of outperforming all other available quantum hardware.

IONQ AND Q CENTER ANNOUNCE PARTNERSHIP TO BRING QUANTUM HARDWARE TO RESEARCHERS AND STUDENTS IN SOUTH KOREA

Researchers and students across South Korea will be able to immediately start running jobs on IonQ's quantum computers. This partnership will enable researchers, scientists, and students to learn, develop, and deploy quantum applications on one of the world's leading quantum systems.

"I am proud to see IonQ enter this alliance with Q Center," said Peter Chapman, CEO & President of IonQ. "IonQ's hardware will serve as the backbone for quantum research. Our technology will play a critical role not only in the advancement of quantum, but also in fostering the next generation of quantum researchers and developers in South Korea."

"WE BELIEVE IONQ HAS THE MOST ADVANCED QUANTUM TECHNOLOGY AVAILABLE, AND THROUGH OUR PARTNERSHIP, WE WILL BE ABLE TO MAKE TREMENDOUS STRIDES IN THE ADVANCEMENT OF THE INDUSTRY."

"Our mission is to cultivate and promote the advancement of quantum information research in South Korea," said SKKU Professor of SAINT (SKKU Advanced Institute of NanoTechnology), Yonuk Chong. "We believe IonQ has the most advanced quantum technology available, and through our partnership, we will be able to make tremendous strides in the advancement of the industry."

This alliance builds on IonQ's continued success. IonQ recently released a product roadmap to deploy rack mounted quantum computers by 2023, and achieve broad quantum advantage by 2025. IonQ also recently unveiled a new $5.5 million, 23,000 square foot Quantum Data Center in Maryland's Discovery District. IonQ has raised $84 million in funding to date, announcing new investment from Lockheed Martin, Robert Bosch Venture Capital GmbH (RBVC) and Cambium earlier this year. Previous investors include Samsung Electronics, Mubadala Capital, GV, Amazon, and NEA. The company's two co-founders were also recently named to the National Quantum Initiative Advisory Committee (NQIAC).

20 Jan 2021

23 Researchers improve data readout by using 'quantum entanglement'

by UNIVERSITY OF YORK

https://www.eurekalert.org/pub_releases/2021-01/uoy-rid012021.php

Researchers say they have been able to greatly improve the readout of data from digital memories – thanks to a phenomenon known as 'quantum entanglement'.

The research team, which included researchers from the Italian Institute of Metrological Research (INRIM) and the University of York, say the findings could have major applications for digital storage devices, including optical memories such as CD or BluRay disks.

This is the first experimental demonstration that quantum sources of light can enhance the readout of information from digital memories, an advance that could potentially lead to faster access of data in large databases and to construct memories with higher capacities in our next-generation computers.

In an optical memory, bits are read by shining a laser beam over the reflecting surface of the disk. In the memory, each microscopic cell has one of two possible levels of reflectivity, representing the values "zero" and "one" of a bit.

As a result, the laser beam reflected from a cell may be more or less intense depending on the value of the bit. The intensity of the beam is then registered by a detector and finally translated into an electrical signal.

However, when the intensity of the laser beam becomes too low, for example as a result of an increased speed of the disk, energy fluctuations prevent the correct retrieval of the bits, introducing too many errors.

The study showed how to fix this problem by resorting to more sophisticated light sources, where the use of quantum entanglement completely removes the unwanted fluctuations.

The researchers say the consequences of the study go far beyond applications to digital memories. In fact, the same principle can be used in spectroscopy and the measurement of biological samples, chemical compounds and other materials.

The scheme also paves the way for non-invasive, ultra-sensitive measurements by greatly reducing the optical power without reducing the amount of information recovered from the systems.

Another promising perspective explored by the researchers is to extend the method to the recognition of complex patterns in conjunction with modern machine-learning algorithms, with potential implications for bio-imaging.

Professor Stefano Pirandola, from the Department of Computer Science at the University of York, said: “This experiment finally shows how we can harness quantum entanglement to better read information from memory devices and other physical systems.”

20 Jan 2021

24 How Quantum Computers Could Usher In a Golden Age of Computing Power

by DANIEL ACKERMAN

https://scitechdaily.com/how-quantum-computers-could-usher-in-a-golden-age-of-computing-power/

Since the 1940s, classical computers have improved at breakneck speed. Today you can buy a wristwatch with more computing power than the state-of-the-art, room-sized computer from half a century ago. These advances have typically come through electrical engineers’ ability to fashion ever smaller transistors and circuits, and to pack them ever closer together.

But that downsizing will eventually hit a physical limit – as computer electronics approach the atomic level, it will become impossible to control individual components without impacting neighboring ones. Classical computers cannot keep improving indefinitely using conventional scaling.

Quantum computing, an idea spawned in the 1980s, could one day carry the baton into a new era of powerful high-speed computing. The method uses quantum mechanical phenomena to run complex calculations not feasible for classical computers. In theory, quantum computing could solve problems in minutes that would take classical computers millennia. Already, Google has demonstrated quantum computing’s ability to outperform the world’s best supercomputer for certain tasks.

But it’s still early days – quantum computing must clear a number of science and engineering hurdles before it can reliably solve practical problems. More than 100 researchers across MIT are helping develop the fundamental technologies necessary scale up quantum computing and turn its potential into reality.

What is quantum computing?

It helps to first understand the basics of classical computers, like the one you're using to read this story. Classical computers store and process information in binary bits, each of which holds a value of 0 or 1. A typical laptop could contain billions of transistors that use different levels of electrical voltage to represent either of these two values. While the shape, size, and power of classical computers vary widely, they all operate on the same basic system of binary logic.

Quantum computers are fundamentally different. Their quantum bits, called qubits, can each hold a value of 0, 1, or a simultaneous combination of the two states. That's thanks to a quantum mechanical phenomenon called superposition. "A quantum particle can act as if it's in two places at once," explains John Chiaverini, a researcher at the MIT Lincoln Laboratory's Quantum Information and Integrated Nanosystems Group.

Particles can also be "entangled" with each other, as their quantum states become inextricably linked. Superposition and entanglement allow quantum computers to "solve some kinds of problems exponentially faster than classical computers," Chiaverini says.

Chiaverini points to particular applications where quantum computers can shine. For example, they're great at factoring large numbers, a vital tool in cryptography and digital security. They could also simulate complex molecular systems, which could aid drug discovery. In principle, quantum computers could turbocharge many areas of research and industry – if only we could build reliable ones.

How do you build a quantum computer?

Quantum systems are not easy to manage, thanks to two related challenges. The first is that a qubit's superposition state is highly sensitive. Minor environmental disturbances or material defects can cause qubits to err and lose their quantum information. This process, called **decoherence**, limits the useful lifetime of a qubit.

The second challenge lies in **controlling the qubit to perform logical functions**, often achieved through a finely tuned pulse of electromagnetic radiation. This manipulation process itself can generate enough incidental electromagnetic noise to cause decoherence. To scale up quantum computers, engineers will have to strike a balance between protecting qubits from potential disturbance and still allowing them to be manipulated for calculations. This balance could theoretically be attained by a range of physical systems, though two technologies currently show the most promise: superconductors and trapped ions.

A **superconducting quantum computer** uses the flow of paired electrons – called "Cooper pairs" – through a resistance-free circuit as the qubit. "A superconductor is quite special, because below a certain temperature, its resistance goes away," says William Oliver, who is an associate professor in MIT's Department of Electrical Engineering and Computer Science, a Lincoln Laboratory Fellow, and the director of the MIT Center for Quantum Engineering.

The computers Oliver engineers use qubits composed of superconducting aluminum circuits chilled close to absolute zero. The system acts as an anharmonic oscillator with two energy states, corresponding to 0 and 1, as current flows through the circuit one way or the other. These superconducting qubits are relatively large, about one tenth of a millimeter along each edge – that's hundreds of thousands of times larger than a classical transistor. A superconducting qubit's bulk makes it easy to manipulate for calculations.

But it also means Oliver is constantly fighting decoherence, seeking new ways to protect the qubits from environmental noise. His research mission is to iron out these technological kinks that could enable the fabrication of reliable superconducting quantum computers. “I like to do fundamental research, but I like to do it in a way that’s practical and scalable,” Oliver says. “Quantum engineering bridges quantum science and conventional engineering. Both science and engineering will be required to make quantum computing a reality.”

Another solution to the challenge of manipulating qubits while protecting them against decoherence is a trapped ion quantum computer, which uses individual atoms – and their natural quantum mechanical behavior – as qubits. Atoms make for simpler qubits than supercooled circuits, according to Chiaverini. “Luckily, I don’t have to engineer the qubits themselves,” he says. “Nature gives me these really nice qubits. But the key is engineering the system and getting ahold of those things.”

Chiaverini’s qubits are **charged ions**, rather than neutral atoms, because they’re easier to contain and localize. He uses lasers to control the ion’s quantum behavior. “We’re manipulating the state of an electron. We’re promoting one of the electrons in the atom to a higher energy level or a lower energy level,” he says.

The ions themselves are held in place by applying voltage to an array of electrodes on a chip. “If I do that correctly, then I can create an electromagnetic field that can hold on to a trapped ion just above the surface of the chip.” By changing the voltages applied to the electrodes, Chiaverini can move the ions across the surface of the chip, allowing for multiqubit operations between separately trapped ions.

So, while the qubits themselves are simple, fine-tuning the system that surrounds them is an immense challenge. “You need to engineer the control systems – things like lasers, voltages, and radio frequency signals. Getting them all into a chip that also traps the ions is what we think is a key enabler.”

Chiaverini notes that the engineering challenges facing trapped ion quantum computers generally relate to qubit control rather than preventing decoherence; the reverse is true for superconducting-based quantum computers. And of course, there are myriad other physical systems under investigation for their feasibility as quantum computers.

Where do we go from here?

If you’re saving up to buy a quantum computer, don’t hold your breath. Oliver and Chiaverini agree that quantum information processing will hit the commercial market only gradually in the coming years and decades as the science and engineering advance.

In the meantime, Chiaverini notes another application of the trapped ion technology he’s developing: highly precise optical clocks, which could aid navigation and GPS. For his part, Oliver envisions a linked classical-quantum system, where a classical machine could run most of an algorithm, sending select calculations for the quantum machine to run before its qubits decohere. In the longer term, quantum computers could operate with more independence as improved error-correcting codes allow them to function indefinitely.

“Quantum computing has been the future for several years,” Chiaverini says. But now the technology appears to be reaching an inflection point, shifting from solely a scientific problem to a joint science and engineering one – “quantum engineering” – a shift aided in part by Chiaverini, Oliver, and dozens of other researchers at MIT’s Center for Quantum Engineering (CQE) and elsewhere.

19 Jan 2021

25 Malwarebytes breached by SolarWinds hackers

by Arielle Waldman

https://searchsecurity.techtarget.com/news/252495069/Malwarebytes-breached-by-SolarWinds-hackers

The nation-state threat actors behind the SolarWinds hack used more than malicious software updates to breach organizations.

In a blog post Tuesday, Malwarebytes disclosed it was targeted by the same threat actors with one major difference: Malwarebytes is not a SolarWinds customer. The antimalware vendor was breached through another vector that is separate from the supply chain attack revealed in December.

"We can confirm the existence of another intrusion vector that works by abusing applications with privileged access to Microsoft Office 365 and Azure Environments," Malwarebytes CEO Marcin Kleczynski wrote in the blog post.

SearchSecurity asked Malwarebytes to expand on what those abused applications are.

"The investigation indicates the attackers leveraged a dormant email protection product within our Office 365 tenant that allows access to a limited subset of internal company emails," Kleczynski said in an email to SearchSecurity.

After an extensive investigation, Malwarebytes determined the "attacker only gained access to a limited subset of internal emails." According to the blog, no evidence of unauthorized access or compromise in any of their internal on-premises and production environments was found.

Initially, Malwarebytes was alerted to the intrusion on Dec. 15 by Microsoft's Security Response Center. According to the blog, the security vendor received information about suspicious activity from a third-party application in its Microsoft Office 365 tenant; the activity was consistent with the tactics, techniques and procedures (TTPs) used by the SolarWinds hackers.

"This investigation indicates the attackers exploited an Azure Active Directory weakness that allowed access to a limited subset of internal company emails. We do not use Azure cloud services in our production environments," Kleczynski wrote.

Microsoft had previously confirmed that it was compromised in connection with the SolarWinds attack on Dec. 31, stating the discovery of one account that had been used to "view source code in a number of source code repositories." According to the blog post, the investigation "found no evidence of access to production services or customer data."

Subsequently, warnings of additional vectors, aside from the SolarWinds Orion platform used in the supply chain attack, were published. In an alert on Jan. 8, the Cybersecurity Infrastructure and Security Agency (CISA) said it detected post-compromise threat activity in Microsoft Cloud environments.

"The Cybersecurity and Infrastructure Security Agency (CISA) has evidence of initial access vectors in addition to the compromised SolarWinds Orion products," the alert said. "This alert addresses activity – irrespective of the initial access vector leveraged – that CISA attributes to an APT actor. Specifically, CISA has seen an APT actor using compromised applications in victim's Microsoft 365 (M365)/Azure environment."

One example of a Microsoft 365 breach occurred inside the Department of Justice (DOJ). On Jan. 6, DOJ spokesman Marc Raimondi issued a statement revealing that threat actors behind the SolarWinds attacks accessed the DOJ's Office 365 email environment.

While additional government agencies, along with tech giants and security vendors, have also been impacted by these nation-state attackers, they were all SolarWinds customers. The Malwarebytes breach represents the growing scope of the cyberespionage campaign.

26 MeitY collaborates with Amazon to set up India's first quantum computing lab

by Prasid Banerjee

https://www.livemint.com/news/india/meity-collaborates-with-amazon-to-set-up-india-s-first-quantum-computing-lab-11611063127192.html

The Ministry of Electronics and Information Technology (MeitY) has announced a collaboration with Amazon Web Services (AWS) to develop a Quantum Computing Applications Lab in the country. The lab is meant to provide access to quantum computing development environment for the developer, scientific and academic communities. “Enabling our scientific community with advanced technologies plays a key role towards scientific advancements and learning,” said Ajay Sawhney, Secretary, MeitY. Amazon will provide hosting with technical and programmatic support for the lab.

According to Rajendra Kumar, Additional Secretary, MeitY, the initiative is a first of its kind in the world and will pave the way for “new discoveries and disruptions”. The government says this new lab will take inputs from Central and State governments, Research Institutions and Academia to identify problem statements in quantum computing. It will also invite applications from researchers and work with subject matter experts. Selected applicants will be provided quantum computing hardware, simulators and programming tools on demand and at no cost, through a quantum computing service called Amazon Braket.

27 The World's Top Ten Quantum Tech Universities and Research Institutions

by Matt Swayne

https://thequantumdaily.com/2021/01/19/the-worlds-top-ten-quantum-tech-universities-and-research-institutions/

University research labs are playing a central role in the development of quantum technologies, such as quantum computers and quantum communication devices. Universities often approach quantum science from a number of angles. Some are good at theoretical approaches to quantum science. Some are strong at applied quantum science. Some focus on the educational and outreach of quantum physics.

Some combine all of these approaches to become powerhouses at quantum science, particularly quantum information science – and well worth it to keep watch on these institutions as the quantum era unfurls.

The following are multi-dimensional quantum powerhouses who are using **research, teaching, or service** – and, in some cases, all three – to build the quantum era. It should be noted that this list shouldn't be seen as a snapshot of a horse race between these institutions or their countries. We used the Nature Index, which measures the largest contributors to papers published in 82 leading journals, as a rough measure of impact. We looked at count (a country/region or an institution is given an AC of 1 for each article that has at least one author from that country/region or institution) and share, which takes into account the share of authorship on each article. There are many other tangible and intangible factors to determine exact leadership that are difficult to ascertain.

Chinese Academy of Science

The Chinese Academy of Sciences is the national academy for the natural sciences of the People's Republic of China. It was established in 1958 in Beijing. It typically ranks in the top 5 of Chinese mainland universities in prestigious ratings, such as U.S. News Report and QS World University.

The university's quantum information sciences is stretched across several institutes, academies, centers and colleges, according to Nature. The Academy's Shanghai Research Center for Quantum Sciences, CAS is the most focused on quantum technology. This center has 11 researchers publish from Oct. 1, 2019 to Sept. 30, 2020 and a 1.43 share in the Nature Index.

One example of quantum research in 2020 includes entanglement-based secure quantum cryptography over 1120 kilometres.

Harvard University

Harvard University – which, like Cher, Madonna, and Bono only needs one name, i.e. Harvard – ranks high in nearly every facet of the quantum technology discovery process: teaching, research and outreach. The Nature Index identifies its overall research input as one of the top in the world. It has a total count of 2540 and a share of 933. The university's physical science share is 195.

The Harvard Quantum Initiative (HQI) is one example of the university's commitment to not just quantum research, but applying that research to confront challenges facing society. The initiative is a community of researchers focused on the advancement of science and engineering of quantum systems and applications.

Led by co-directed by professors John Doyle, Evelyn Hu, and Mikhail Lukin, the mission is to "help scientists and engineers explore new ways to transform quantum theory into useful systems and devices."

Max Planck Society

The Max Planck Society is not technically a university. It's a non-profit confederation of 86 research institutions and facilities that conduct basic research in the natural sciences, life sciences and humanities. It also operates another 20 Max Planck Centers with research institutions such as the Princeton University in the USA, the Paris University Science Po in France, the University College London in UK, and the University of Tokyo in Japan.

A good example of the quantum science spearheaded by the society is the Max Planck Institute of Quantum Optics. According to the Nature Index, the institute has a count of 95 and a share of 21.56. A key study released last year was "Many-body Topological Invariants From Randomized Measurements in Synthetic Quantum Matter," which was published in April, and Long-Distance Distribution of Atom-Photon Entanglement at Telecom Wavelength, published in January 2020.

Overall, Max Planck Society has an index count of 2730 and a share of 795.

Stanford University

As an undisputed giant in technology – Google got its start there – Stanford is a growing giant in quantum technology.

A lot of great work in quantum information science is coming from Stanford's Institute for Theoretical Physics. Members of the institute are investigating the full length of quantum science's deepest mysteries and include advances in quantum computing.

According to the institute: "Quantum information researchers at SITP have played an important role in the development of the basic theory of quantum communication. They continue to search for better ways to protect quantum computers from noise and communications from prying eavesdroppers. A unique feature of the quantum information group at SITP, however, is its close integration and participation in research on quantum gravity and black holes. Stanford is at the forefront of exploring the role of quantum entanglement to the geometry of space, the importance of quantum error correction in black hole evaporation, and even the relevance of computational complexity to stability of space."

According to Stanford's output, as registered by Nature, the university has an index count of 1693 and a share of 655. In the physical sciences alone, Nature Index shows a 225 share in the physical sciences, where you're likely to find many quantum projects.

Helmholtz Association of German Research Centres

This is the biggest research organization in Germany. Based on its Nature Index score, it's a leading global powerhouse in research with a count of 2442 and a share of 551 – 271 share is in the physical sciences.

According to The Helmholtz Association, its mission for quantum is "to contribute to solving important and urgent social, scientific, and economic problems." The association is continually working to advance the development of quantum technologies. Those efforts run the complete cycle of research, from basic research to system development to application.

As an example faculty member Forschungszentrum Jülich, one of the association's research center, part of the international team that contributed to Google's demonstration of quantum supremacy in 2019.

University of Maryland

Several major quantum initiatives places the University of Maryland, College Park (UMCP) on the list of global quantum research powerhouses. Its Nature Index count is 672 and has a share of about 164. The physical sciences represent a major part of that share, or 91.61.

One sign of its leadership in quantum is the The Joint Center for Quantum Information and Computer Science (QuICS), which is a partnership between the University of Maryland (UMD) and the National Institute of Standards and Technology (NIST). The center advances research and education in quantum computer science and quantum information theory.

University of Science and Technology China

The Chinese equivalent of the Ivy League is called, the C9 League. The University of Science and Technology of China is a national research university in Hefei, Anhui, China, is one of the top members of the C9 League.

Its Nature Index speaks for itself. It has a 1307 count and a 474 share. About 179 of that share rests in the physical sciences.

The university's quantum technology research is legend, particularly in quantum communication. A recent study demonstrated the ability to maintain entanglement-based secure quantum cryptography over 1120 kilometers.

University of Cambridge

Perched at the apex of the UK's golden triangle, the University of Cambridge is at the apex of the country's pioneering quantum movement. Several quantum computing startups have spun out of the university, while many other quantum organizations made their homes near Cambridge because of the ready access to world-leading talent and brainpower.

The Centre for Quantum Information and Foundations is an example of the university's ability to combine research, teaching and service to encourage the growth of this ecosystem. Based in the Department for Applied Maths and Theoretical Physics, the centre "conducts theoretical research into all aspects of quantum information processing, the implications of quantum computing and quantum information theory for physics, and broader foundational questions in quantum physics."

In the Nature Index, the University of Cambridge has a 1395 count and a 450 share. Physical science claims a 175 of that share.

University of Waterloo

A pioneer in quantum computing, the University of Waterloo in Canada is acknowledged as a triple-crown winner in quantum science. It shines as a quantum educator, a quantum research hub, and as a good member of the ecosystem that's committed to using outreach and startup development to make sure quantum technology reaches the public.

The university's quantum crown jewel is The Institute for Quantum Computing (IQC). This scientific research institute proves "the quantum laws of nature in order to develop powerful new technologies and drive future economies."

Nature Index pegs the University of Waterloo with a Count of 191 and a Share of 71, with the Physical Sciences representing about a 33 share.

A good example of University of Waterloo's quantum research in action is its recent use of a mirror for quantum research being used to possibly identify counterfeit cash.

University of Chicago

Chicago is a hub of many industries in the United States. It's apparent that it is growing as a quantum hub. At least one of the reasons why quantum scientists and entrepreneurs are flocking to this midwestern metropolis is its universities. One of the most prestigious research-heavy universities is the University of Chicago.

The university is a leader in the Chicago Quantum Exchange, which is fostering the growing quantum ecosystem in the midwest – and beyond.

On the Nature scale, U-of-C has a count of 722 and a share of 253, with 89 of that share in the physical sciences.

28 New and Hardened Quantum Crypto System Notches “Milestone” Open-Air Test

by Jeremy Hsu

https://spectrum.ieee.org/tech-talk/computing/hardware/quantum-crypto-mdi-qkd-satellites-security

Quantum cryptography remains the ostensibly impervious technology for which new hacks and potential vulnerabilities continue to be uncovered – perhaps ultimately calling into question its alleged unhackability.

Yet now comes word of a successful Chinese open-air test of a new generation quantum crypto system that allows for untrustworthy receiving stations.

The previous iteration of quantum cryptography did not have this feature. Then again, the previous iteration did have successful ground and satellite experiments, establishing quantum links to transmit secret messages over hundreds of kilometers.

The present new and more secure quantum crypto system is, perhaps not surprisingly, much more challenging to implement.

It creates its secret cryptographic keys based on the quantum interference of single photons – light particles – that are made to be indistinguishable despite being generated by independent lasers. As long as sender and receiver use trusted laser sources, they can securely communicate with each other regardless of whether they trust the detectors performing the measurements of the photons’ quantum interference.

Because the cryptographic key can be securely transmitted even in the case of a potentially hacked receiver, the new method is called **measurement-device independent quantum key distribution (MDI-QKD)**.

“It is not far-fetched to say that MDI-QKD could be the de-facto [quantum cryptography] protocol in future quantum networks, be it in terrestrial networks or across satellite communications.” says Charles Ci Wen Lim, an assistant professor in electrical and computer engineering and principal investigator at the Centre for Quantum Technologies at the National University of Singapore; he was not involved in the recent experiment.

In their unprecedented demonstration, Chinese researchers figured out how to overcome many of the experimental challenges of implementing MDI-QKD in the open atmosphere. Their paper detailing the experiment was published last month in the journal Physical Review Letters.

Such an experimental system bodes well for future demonstrations involving quantum links between ground stations and experimental quantum communication satellites such as China’s Micius, says Qiang Zhang, a professor of physics at the University of Science and Technology of China and an author of the recent paper.

The experiment demonstrated quantum interference between photons even in the face of atmospheric turbulence. Such turbulence is typically stronger across horizontal rather than vertical distances. The fact that the present experiment traverses horizontal distances bodes well for future ground-to-satellite systems. And the 19.2-kilometer distance involved in the demonstration already exceeds that of the thickest part of the Earth’s atmosphere.

To cross so much open air, the Chinese researchers developed an adaptive optics system similar to the technology that helps prevent atmospheric disturbances from interfering with astronomers’ telescope observations.

Even MDI-QKD is not 100% secure – it remains vulnerable to hacking based on attackers compromising the quantum key-generating lasers. Still, the MDI-QKD security scheme offers, Zhang claims, “near perfect information theoretical security.” It’s entirely secure, in other words, in theory.

The remaining security vulnerabilities on the photon source side can be “pretty well taken care of by solid countermeasures,” Lim says. He and his colleagues at the National University of Singapore described one possible countermeasure in the form of a “quantum optical fuse” that can limit the input power of untrusted photon sources. Their paper was recently accepted for presentation during the QCRYPT 2020 conference.

All in, Lim says, the Chinese team’s “experiment demonstrated that adaptive optics will be essential in ensuring that MDI-QKD works properly over urban free-space channels, and it represents an important step towards deploying MDI-QKD over satellite channels.” From his outside perspective, he described the Chinese team’s work as a “milestone experiment for MDI-QKD.”

18 Jan 2021

29 All About Encryption Backdoors

by Mark Vojtko

https://www.thesslstore.com/blog/all-about-encryption-backdoors/

We Examine the Double-Edged Swords of the Cybersecurity World

It’s not in your pocket. Not in the car. Not in your bag. Where could your key be? You need a way to get in your place. So, you call a locksmith, who can use his tools to provide another way inside.

But what if we’re talking encryption instead? There are no locksmiths in the cryptography world. What gets encrypted stays encrypted (unless you’re the owner). Theoretically, at least. One exception to that rule is encryption backdoors.

Encryption backdoors are a simple concept. Think of them like the spare key you hide under the rock in your yard. They’re a weakness that allows for entry in case of a loss of access or an emergency. They can be maliciously created by malware or intentionally placed in either hardware or software. There has been much debate about encryption backdoors because the two main debaters are viewing the issue from very different perspectives. On one hand, they allow for a way in if the situation requires it. But on the other hand, they can and most likely will be found by attackers.

So how do encryption backdoors work exactly? In what circumstances have they been used in the past? And what are the arguments for and against their deployment?

What is an Encryption Backdoor?

An encryption backdoor is any method that allows a user (whether authorized or not) to bypass encryption and gain access to a system. Encryption backdoors are similar in theory to vulnerabilities, especially with regards to functionality. Both offer a non-standard way for a user to enter a system as they please. The difference lies in the human train of thought behind them. Encryption backdoors are deliberately put in place, either by software developers or attackers. Vulnerabilities, however, are accidental in nature.

In the world of cyberthreats, backdoors are among the most discreet kind. They're the polar opposite of something like ransomware, which is the cyber-equivalent of grabbing the user and slapping them in the face repeatedly. Encryption backdoors are well hidden, lurk in the background, and are only known by a very small group of people. Only the developers and a handful of select users that require the capabilities that the backdoor provides should be aware of its existence.

The power and versatility of backdoors has made them very popular among cybercriminals. In fact, a 2019 study by Malwarebytes found that backdoors in general, including encryption backdoors, were number four on the list of most common threats faced by both consumers and businesses. The report also discovered that the use of backdoors is on the rise, with a 34% increase in detections for consumers and a whopping 173% increase for businesses, compared to the previous year. Considering encryption backdoors are one of the primary types of backdoors, their use is no doubt on the rise, as well.

It's more important than ever to be aware of encryption backdoors and how they work. Since they can be used for either good or evil, it's not always the most straightforward subject. Let's look at both sides of the coin by taking a closer at the different ways they are put into practice.

How Are Encryption Backdoors Used?

Some backdoors are are intended to help users, and others are intended to hurt them. We're going to classify backdoors into two primary types based on the result they're designed to achieve – malware backdoors and built-in backdoors.

Malware Backdoors

We'll start with the bad guys first. They create backdoor malware for nefarious means, such as stealing personal data, accessing your financial records, loading additional types of malware onto your system, or completely taking over your device.

Backdoor malware is considered a type of Trojan, which means that it aims to disguise itself as something completely different from its true form. You may think you're downloading a regular old Word document or a trusted piece of software from a file-sharing site, but you're actually getting something that's going to open up a backdoor on your system that an attacker can use to access whenever they want.

Backdoor malware, like Trojans, can also be capable of copying itself and distributing the copies across networks to other systems. They can do this all automatically without any input required from the hacker.

These backdoors can then be used as a means to an end for further attacks, such as:

- Spyware
- Keyloggers
- Ransomware
- Cryptojacking
- Using your PC in a DDOS attack

For instance, maybe you download a free file converter. You go to use it and it doesn't seem to work properly (spoiler alert – it was never intended to) so you go and uninstall it from your system. Unbeknownst to you though, the converter was actually backdoor malware, and you now have a wide-open backdoor on your system.

Attackers can go a step further and create a backdoor using a functional piece of software. Perhaps you downloaded a widget that displays regularly updated stock prices. You install it and it works just fine. Nothing seems amiss. But little did you know, it also opened a backdoor on your machine.

For cybercriminals, that's usually just the first step –getting their foot in the door. A common avenue for hackers to go down at this point is deploying a rootkit. The rootkit is a collection of malware that serves to make itself invisible and conceal network activity from you and your PC. Think of a rootkit like a doorstop that keeps the point of access open to the attacker.

Rootkits and backdoor malware in general can be difficult to detect, so be careful when browsing, avoid files from unknown or untrusted sources, keep your applications & OS updated, and take advantage of anti-virus and anti-malware programs.

Built-In Backdoors

It's not all bad when it comes to encryption backdoors, however. As we touched on, they can be used for ethical purposes, too. Perhaps a user is locked out of critical information or services and doesn't have any other way to get in. An encryption backdoor can restore access. They can also be of help when troubleshooting software issues, or even be used to access information that can help solve crimes or find a missing person or object.

Built-in backdoors are purposely deployed by hardware and software developers, and they aren't usually created with nefarious means in mind. Oftentimes they're simply part of the development process. Backdoors are used by developers so they can more easily navigate the applications as they're coding, testing, and fixing bugs. Without a backdoor, they'd have to jump through more hoops like creating a "real" account, entering personal information that's usually required for regular users, confirming their email address, etc.

Backdoors like these aren't meant to be part of the final product, but sometimes they get left in by accident. As with a vulnerability, there's a chance that the backdoor will be discovered and used by attackers.

The other main category of built-in backdoors is those that are requested by national governments and intelligence agencies. The governments of the Five Eyes (FVEY) intelligence alliance, Australia, Canada, New Zealand, the United Kingdom, and the United States, have repeatedly requested that tech and software companies install backdoors in their products. Their rationale is that these backdoors can help find critical evidence for use in criminal investigations. Apple, Facebook, and Google have all said no to these requests.

If a company does agree to installing a backdoor however, then it usually happens somewhere in the supply chain, where it is appropriately referred to as a "supply chain backdoor." It's because it occurs during the manufacturing and/or development process when the components of the product are still floating around at some point in the supply chain. For instance, a backdoor could be loaded onto a microprocessor at the chip maker's facility, whereafter it gets sent to various OEMs for use in consumer products. Or it could be loaded as the finished product is being sent to the consumer. For example, a government agency could intercept a shipment of devices meant for an end-user and load a backdoor via a firmware update. Encryption backdoors can be installed with the knowledge of the manufacturer or done covertly.

Supply chain backdoors can occur during the software development process, as well. Open-source code has many advantages for developers, saving time and resources instead of reinventing the wheel. Functional and proven libraries, applications, and development tools are created and maintained for the greater good, free for all to use. It has proven to be an efficient and powerful system.

Except, of course, when a backdoor is intentionally planted somewhere. Contributions to open-source code are always subject to review and scrutiny, but there are times when a malicious backdoor can slip through the cracks and make its way out to developers and eventually users. In fact, GitHub found in a 2020 report that nearly one in five software bugs were intentionally created for malicious purposes.

Encryption Backdoors in the Real World

Let's take a look at some of the most significant and well known instances of encryption backdoors, and the consequences associated with their use:

- **1993 – Clipper Chip** – While there were previous encryption backdoors prior to this, the Clipper Chip of 1993 was the first to gain major mainstream attention. The chip was an effort by the NSA to create a security system that, while sufficiently secure, could also be cracked at will by investigators if the need arose. The way it worked was that an 80-bit key was burned into the chip as it was manufactured. A copy of that key was held in escrow, and government agents with sufficient clearance could access it. The concept was met with heavy resistance within the industry, never quite got off the ground, and was dead within a few years.

- **2005 – Sony BMG** – A decade and a half ago, while you were busy listening to 50 Cent or Mariah Carey, Sony was shipping millions of CD's containing a rootkit. Intended as a copyright protection measure, it would automatically install itself on your PC when the CD was inserted. Not only did it try and prevent you from burning CDs, but it also spied on your listening habits and opened a backdoor on your machine. Sony faced a wave of lawsuits as a result, recalling the CDs in question and paying out millions in damages.

- **2013 – Edward Snowden** – One of the many revelations that came as a result of Snowden's leaks was that the government had, in numerous instances, intercepted network gear en route to an end user and loaded compromised firmware on it. The firmware, of course, contained a backdoor that the NSA could (and often did) use to gain access to the user's network.

- **2014 – Emotet** – A malware strain, and more specifically a banking Trojan, Emotet is essentially an information stealer. It was originally intended for gathering sensitive financial data but is now used primarily as a backdoor. As of 2019, it was still one of the most prevalent threats in cyberspace and is commonly used as a starting point for launching ransomware attacks.

- **2015 – Apple** – Apple has continuously refused to put backdoors in their products, despite repeated requests from the US government. The most high-profile instance happened in 2015, following the San Bernardino terrorist attacks. The FBI found an iPhone that was owned by one of the perpetrators and asked Apple to help unlock it. Apple said no and even made a concerted effort to make their devices harder to crack moving forward. The FBI was eventually able to use a third-party to access the phone.

- **2017 – WordPress Plugins** – An SEO scam in 2017 ended up affecting over 300,000 WordPress sites, revolving around a WordPress plugin "Simply WordPress." It was a CAPCHA plugin that did more than advertised, unfortunately. It came with a "feature" that opened a backdoor that provided admin access to the site it was installed on.

The Debate About Encryption Backdoors

The debate around the existence of encryption backdoors, and particularly built-in backdoors, has been raging on for decades. Thanks to the "shades of grey" nature of their intended and actual uses, the debate shows no sign of slowing down anytime soon. Especially considering that the main proponent of encryption backdoors, national governments, is also the only party that could legally outlaw them. So, what are the two sides of the argument?

The Pros of Encryption Backdoors

The members of the Five Eyes alliance argue that built-in encryption backdoors are a must for maintaining national and global security. Then-FBI Director Christopher Wray attempted to sum up the US government's position in 2018, explaining

"We're not looking for a 'back door' – which I understand to mean some type of secret, insecure means of access. What we're asking for is the ability to access the device once we've obtained a warrant from an independent judge, who has said we have probable cause."

Government officials often point out that what they truly desire is more like a "front door" that can grant access and decryption only in situations that meet certain criteria. The theory is that it would be something only the "good guys" can use.

Those in favor of backdoors argue that the technological gap between the authorities and cybercriminals is growing, and that the legal and technological powers of law enforcement agencies aren't currently enough to keep up. Hence, the need for a shortcut, a secret way in.

In other instances, authorities simply need access to gain evidence and information regarding a case. Numerous criminal investigations have been held up because locked phones couldn't be accessed. And after all, isn't the information in a phone the kind that police would normally have the right to access with a search warrant?

Key Escrow Backdoors

A common solution that is proposed by supporters of built-in backdoors is the use of what's called a "key escrow" system. The concept is that a trusted third party would act as a secure repository for keys, allowing for decryption if law enforcement can get legal permission to do so.

Key escrow is often used internally by companies in case access to their own data is lost. When it comes to public use though, it's a system that is challenging and costly to implement. There's also a large security risk, since all an attacker would need to do to decrypt something is gain access to the key storage location.

The Cons of Encryption Backdoors

A "front door" for the good guys sounds great in theory. The problem is, functionally, there isn't much difference between that and an encryption backdoor. A hacker will be able to find their way in if it exists, no matter what you want to call it. It's for this reason that most of the big tech companies don't want encryption backdoors in their products. Because then they will be putting their brand name on insecure products that come with out-of-the-box vulnerabilities.

Even if the manufacturer and/or the government are the only ones to initially know about the backdoor, it's inevitable that attackers will eventually discover it. On the large scale, a proliferation of backdoors would almost certainly result in an increase of cybercrimes and create a massive black market of exploits. There could be severe and far-reaching impacts for the public-at-large. For instance, utility infrastructure and critical systems could suddenly be left wide open to attacks from threats both at home and abroad.

There is also the question of privacy when it comes to encryption backdoors. If backdoors are everywhere, then suddenly a government can eavesdrop on citizens and view their personal data as they wish. Even if they didn't at first, the possibility is still there, and it's a slippery slope that gets more slippery with time. A hostile and immoral government, for example, could use a backdoor to locate dissidents that are speaking out against the regime and silence them.

Overall, when it comes to encryption, there's a few basics that are absolutely required in order for it to be effective:

- The data can't be decrypted without the decryption key
- The decryption key can only be accessed by the owner

Backdoors compromise the second point (and in some cases the first), and in that sense they defeat the entire purpose of encrypting data in the first place.

The Future of Encryption Backdoors

The refusal of the giant technology companies to grant encryption backdoors, particularly Apple's actions in 2015, has thus far prevented the setting of any legal precedents for backdoors. If any of them had acquiesced, then more encryption backdoors would have no doubt been created moving forward. While encryption backdoors can result in positive outcomes in certain cases, they also come at the price of exposing our devices to greater risk of attack.

These risks are already increasing, independent of backdoors, thanks to the Internet of Things and proliferation of "smart" devices all over our homes and workplaces. An attacker could compromise an IoT device and work their way up the chain of connections to your own PC, and backdoors make it even easier.

In one corner, you have security experts and privacy advocates in favor of maintaining the strongest possible encryption measures and practices. In the opposite corner you have governments that want backdoors to help solve crimes and maintain public safety. The discussion shows no signs of slowing up and will most likely intensify as technology continues to evolve and spread.

Either way, you and I must continue to protect our own data as best we can. We can't necessarily prevent an attack via a built-in backdoor that we don't even know exists, but we can employ an intelligent mix of security software and best practices to help mitigate the risk of malware backdoors. Make sure your data is encrypted with an encryption algorithm you trust, and that you have full control over the encryption key. If there's a possibility that someone else has a key for your data, then it's not secure.

30 Using drones to create local quantum networks

by Bob Yirka

https://phys.org/news/2021-01-drones-local-quantum-networks.html

A team of researchers affiliated with several institutions in China has used drones to create a prototype of a small airborne quantum network. In their paper published in the journal Physical Review Letters, the researchers describe sending entangled particles from one drone to another and from a drone to the ground.

Computer scientists, physicists and engineers have been working over the last several years toward building a usable quantum network – doing so would involve sending entangled particles between users and the result would be the most secure network ever made. As part of that effort, researchers have sent entangled particles over fiber cables, between towers and even from satellites to the ground. In this new effort, the researchers have added a new element – drones.

To build a long-range quantum network, satellites appear to be the ideal solution. But for smaller networks, such as for communications between users in the same city, another option is needed. While towers can be of some use, they are subject to weather and blockage, intentional or otherwise. To get around this problem, the researchers used drones to carry the signals.

The work involved building a small laser-generating device and affixing it to one of the drones. As it fired, photons were split in two, creating entangled pairs. One of the paired photons was directed toward another drone while the other was directed to a ground station. The drone that received the entangled photon served only as a relay – after refocusing, the photon was forwarded to a third drone, which then sent it to a second ground station. Motorized devices were used on the drones to ensure transmitters and received lined up properly for transmission of the entangled photons.

In the prototype, the photons were sent just one kilometer, but the researchers suggest that moving the drones higher would allow for transmission over distances up to 300 kilometers. They suggest the technology could also be adapted to include moving vehicles on the ground. They further note both the drones and the ground stations could also be connected to a network that included satellites. And they also point out their work was the first to send entangled particles between two moving devices.

16 Jan 2021

31 Intel, Cybereason Beat Ransomware With Hardware Shield

by Jessica Lyons Hardcastle

https://www.sdxcentral.com/articles/news/intel-cybereason-beat-ransomware-with-hardware-shield/2021/01/

Intel and security software vendor Cybereason will provide ransomware protection at the CPU level in a joint product that combines Intel's new Hardware Shield technology, built into its upcoming vPro processors, with Cybereason's anti-ransomware capabilities.

While the ransomware protection isn't yet available – Intel just launched its 11th Core vPro mobile processors this week at CES – it represents the first instance where PC hardware plays a direct role in protecting enterprise endpoints against ransomware, the companies say.

The new vPro processors come with Intel Hardware Shield built into them. This is essentially a bundle of security capabilities including Intel Threat Detection Technology (Intel TDT), which enables security ISVs to offload memory scanning, artificial intelligence (AI)-based malware detection, and other performance-intensive security workloads. Other Hardware Shield features include hardware-accelerated virtualization and encryption to protect applications, data, and operating systems without hurting user productivity.

Cybereason is the first software vendor to integrate the new technology into its security platform. The endpoint security vendor has been investing heavily in anti-ransomware capabilities since 2016, CTO Yonatan Striem-Amit said.

“As part of that, we started engaging with Intel,” he said. “Intel did two things that, for us, were very interesting in these 11th generation CPUs.”

Cybereason Platform With Intel Hardware Shield

The first is the embedded GPU, which allows the platform to offload machine learning models and other more advanced, performance-intensive anti-ransomware technologies onto the GPU when it’s idle. “If you try to run those on a regular CPU without acceleration, it may cause some performance impact for the user,” Striem-Amit said. “By leveraging the GPU capabilities, we should be able to run these more complex, advanced models without any risk to the overall user experience.”

The second thing involves using the CPU performance monitoring unit (PMU) to detect ransomware. The Intel PMU sits beneath applications, the OS, and virtualization layers, and it generates signals that report on CPU activity. But it can also detect threats in real time. “What Intel and us have discovered, is that using these signals we’re able to tell if there is a massive amount of encryption happening,” Striem-Amit said.

As it detects threats, Intel TDT sends a signal that can then trigger remediation. Integrating Intel TDT into the Cybereason Defence Platform provides another source of ransomware threat detection, Striem-Amit said.

“Using that (TDT) signal, along with the rest of our behavioral analysis components, we are able to say with greater confidence that right now there is ransomware potentially happening in the customer’s environment,” Striem-Amit said.

Cybereason Says Double-Extortion Ransomware on the Rise

Ransomware protection takes on a whole new level of urgency in 2021 following the huge spike in attacks and skyrocketing, multi-million-dollar ransom demands we saw last year and the first ransomware-related death at a German hospital.

“We’re seeing the ransomware authors continually evolve their code to become better at extracting money,” Striem-Amit said. “Over the last year we’ve seen many more cases of double extortion, which is particularly nefarious because the criminals are causing even more damage to the enterprise victims.”

Double-extortion ransomware attacks weren’t widely used until 2020, according to Check Point’s 2020 mid-year report. In these attacks, hackers first extract large amounts of sensitive data prior to encrypting a victim’s databases. They then threaten to publish that data unless the victim pays ransom demands, thus putting extra pressure on organizations to pay up. A Q3 Check Point report saw another sharp rise in double-extortion ransomware attacks with the security vendor’s threat researchers reporting a 50% increase in the daily average of ransomware attacks, compared to the first half of the year. The vendor expects to see another ransomware uptick in 2021.

And while $10-billion ransoms and double-extortion ransomware didn't really take off until 2020, the threat has been around for a while now, and Cybereason has focused on developing anti-ransomware technology for the last five years, Striem-Amit said.

Ransomware 'Hurts Everyone'

"Since 2016, Cybereason observed the threat of ransomware becoming critical, and we, in a sense, took personal offense because it's hurting everyone, from consumers to our enterprise customers in ways that were debilitating. And it's heartbreaking to talk to a grandmother who lost pictures of her grandkids. This is as dramatic, if not more, than talking to a business who might go down because they have lost all their data and now required to pay this exuberant amount of money. So we made a commitment to go all in on protection against ransomware."

This started with a free product for consumers, called RansomFree, and over the years Cybereason has built out its ransomware prevention technology. The vendor's approach combines intelligence-based, deception, behavioral analytics, and machine-learning algorithms to block ransomware before any data can be encrypted or compromised. This includes protection from attacks leveraging previously unknown, fileless, and master boot record-based ransomware.

"We've developed a lot of technology that not only finds known ransomware but really focuses on unknown ransomware by looking at behavior of a system," Striem-Amit said. "If any program in the operating system is starting to exhibit ransomware-like behavior, we will block it and prevent any damage from being done to your endpoints."

The new anti-ransomware product in development with Intel also follows Cybereason's recent push into extended detection and response (XDR) and a new Breach Protection Warranty that provides up to $1 million in coverage to customers in the event of a breach.

15 Jan 2021

32 Scientists' discovery is paving the way for novel ultrafast quantum computers

by Estonian Research Council

https://phys.org/news/2021-01-scientists-discovery-paving-ultrafast-quantum.html

Scientists at the Institute of Physics of the University of Tartu have found a way to develop optical quantum computers of a new type. Central to the discovery are rare earth ions that have certain characteristics and can act as quantum bits. These would give quantum computers ultrafast computation speed and better reliability compared to earlier solutions. The University of Tartu researchers Vladimir Hizhnyakov, Vadim Boltrushko, Helle Kaasik and Yurii Orlovskii published the results of their research in the scientific journal Optics Communications.

While in ordinary computers, the units of information are binary digits or bits, in quantum computers the units are quantum bits or qubits. In an ordinary computer, information is mostly carried by electricity in memory storage cells consisting of field-effect transistors, but in a quantum computer, depending on the type of computer, the information carriers are much smaller particles, for example ions, photons and electrons. The qubit information may be carried by a certain characteristic of this particle (for example, spin of electron or polarization of photon), which may have two states. While the values of an ordinary bit are 0 or 1, also intermediate variants of these values are possible in the quantum bit. The intermediate state is called the superposition. This property gives quantum computers the ability to solve tasks, which ordinary computers are unable to perform within reasonable time.

Qubits of mixed-ion crystals

Researchers of the Institute of Physics of the University of Tartu showed that microcrystals, synthesized on the basis of mixed optical fluoride crystal matrices doped with erbium, praseodymium and some other ions of rare earth elements, can work as qubits that enable ultrafast optical quantum computing.

Professor Vladimir Hizhnyakov, member of the Estonian Academy of Sciences, says that when selecting the ions, their electronic states of very different properties are of utmost importance. "They must have at least two states in which the ion interaction is very weak. These states are suitable for basic quantum-logic operations on single quantum bits. In addition, a state or states are needed in which the ion interaction is strong – these states enable quantum-logic operations with two or more qubits. All these states must have a long (milli- or microsecond) lifetime and optical transitions must be allowed between these states," Hizhnyakov explained.

He says that so far, finding such electronic states of rare earth ions was not considered possible, and that is why scientists have not looked for such states suitable for qubits among them. "So far, mostly the spin states of atomic nuclei have been studied for the role of qubits. However, their frequency is a million times lower than the frequency of our quantum bits. This is why also quantum computers created on the basis of these qubits would be significantly slower than computers with our electronic states-based quantum bits," he explained.

Higher speed and fewer errors

An ultrafast working cycle would allow, according to Hizhnyakov, to overcome one the major obstacles in the creation of quantum computers. Qubits are namely very sensitive to their environment, which is why any environmental interference may lead to errors in quantum computation. "The coherence time of qubits, i.e. the duration of the pure quantum state, is very short. The faster the computation cycle, the less interference is caused by the surrounding environment in the work of qubits," Hizhnyakov explained.

It has been ascertained that the spectral hole-burning method, previously developed at the Institute of Physics of the University of Tartu can be used for selecting a set of qubits in a microcrystal acting as a computer instance. According to Hizhnyakov, this at present one of most powerful methods of optical spectroscopy, which allows to find those ions in a microcrystal that are the most suitable for use as computer qubits.

Although it is still a long way full of obstacles to an actually working quantum computer, researchers of the laser spectroscopy laboratory of the University of Tartu have started building a pilot prototype of quantum computer based on the new method. According to the researchers, they are on the threshold of presenting the work of the basic elements of the new type of quantum computer.

The completed research study is a part of the joint project "Spectroscopy of entangled states of clusters of rare-earth impurity ions for quantum computing," conducted by the Laboratory of Laser Spectroscopy and the Laboratory of Solid State Theory at the Institute of Physics of the University of Tartu.

33 Cell Phone Location Privacy

by Bruce Schneier

https://securityboulevard.com/2021/01/cell-phone-location-privacy/

We all know that our cell phones constantly give our location away to our mobile network operators; that's how they work. A group of researchers has figured out a way to fix that. "Pretty Good Phone Privacy" (PGPP) protects both user identity and user location using the existing cellular networks. It protects users from fake cell phone towers (IMSI-catchers) and surveillance by cell providers.

It's a clever system. The players are the user, a traditional mobile network operator (MNO) like AT&T or Verizon, and a new mobile virtual network operator (MVNO). MVNOs aren't new. They're intermediaries like Cricket and Boost.

Here's how it works:

(i) **One-time setup:** The user's phone gets a new SIM from the MVNO. All MVNO SIMs are identical.

(ii) **Monthly:** The user pays their bill to the MVNO (credit card or otherwise) and the phone gets anonymous authentication (using Chaum blind signatures) tokens for each time slice (e.g., hour) in the coming month.

(iii) **Ongoing:** When the phone talks to a tower (run by the MNO), it sends a token for the current time slice. This is relayed to a MVNO backend server, which checks the Chaum blind signature of the token. If it's valid, the MVNO tells the MNO that the user is authenticated, and the user receives a temporary random ID and an IP address. (Again, this is now MVNOs like Boost already work.)

(iv) **On demand:** The user uses the phone normally.

The MNO doesn't have to modify its system in any way. The PGPP MVNO implementation is in software. The user's traffic is sent to the MVNO gateway and then out onto the Internet, potentially even using a VPN.

All connectivity is data connectivity in cell networks today. The user can choose to be data-only (e.g., use Signal for voice), or use the MVNO or a third party for VoIP service that will look just like normal telephony.

The group prototyped and tested everything with real phones in the lab. Their approach adds essentially zero latency, and doesn't introduce any new bottlenecks, so it doesn't have performance/scalability problems like most anonymity networks. The service could handle tens of millions of users on a single server, because it only has to do infrequent authentication, though for resilience you'd probably run more.

14 Jan 2021

34 Pivotal discovery in quantum and classical information processing

https://www.swissquantumhub.com/pivotal-discovery-in-quantum-and-classical-information-processing/

Researchers in the Argonne National Laboratory and Pritzker School of Molecular Engineering have demonstrated a novel approach that allows real-time control of the interactions between microwave photons and magnons, potentially leading to advances in electronic devices and quantum signal processing.

Microwave photons are elementary particles forming the electromagnetic waves that we use for wireless communications. Magnons are the elementary particles forming what scientists call spin waves – wave-like disturbances in an ordered array of microscopic aligned spins that can occur in certain magnetic materials.

Microwave photon-magnon interaction has emerged in recent years as a promising platform for both classical and quantum information processing.

The team employs an electrical signal to periodically alter the magnon vibrational frequency and thereby induce effective magnon-photon interaction. The result is a first-ever microwave-magnonic device with on-demand tunability. Before this work, the interaction had proved impossible to manipulate in real time.

The team's device can control the strength of the photon-magnon interaction at any point as information is being transferred between photons and magnons. It can even completely turn the interaction on and off. With this tuning capability, scientists can process and manipulate information in ways that far surpass present-day hybrid magnonic devices.

35 Researchers conduct security analysis and improve quantum random number generation

by University of Science and Technology of China

https://phys.org/news/2021-01-analysis-quantum-random.html

Recently, the research team led by academician GUO GuResearchers in the Argonne National Laboratory and Pritzker School of Molecular Engineering have demonstrated a novel approach that allows real-time control of the interactions between microwave photons and magnons, potentially leading to advances in electronic devices and quantum signal processing.

Microwave photons are elementary particles forming the electromagnetic waves that we use for wireless communications. Magnons are the elementary particles forming what scientists call spin waves – wave-like disturbances in an ordered array of microscopic aligned spins that can occur in certain magnetic materials.angcan from the University of Science and Technology of China of the Chinese Academy of Sciences has made security analysis and improvement of source independent quantum random number generators with imperfect devices.

By studying the actual characteristics of the measurement devices of the source-independent quantum random number generation, the researchers pointed out that the security issues were caused by afterpulse, detection efficiency mismatching, poor sensitivity to photon number distribution in measurement devices, etc., and gave the corresponding solutions.

The source-independent quantum random number generation protocol is a new quantum random number protocol proposed in 2016. This protocol can generate secure random numbers under the condition that the light source is completely untrusted by monitoring the error code of the mutual unbiased basis corresponding to the base of the random number generation. It can simultaneously meet the requirements of security and high rate of random number generator, and has a very high devices loss tolerance.

However, the protocol has some security problems, such as the failure to consider the afterpulse problem of the detector, the mismatch of detection efficiency, the poor sensitivity of the detector to the distribution of light source and other characteristics, which impedes the application of this protocol.

In this study, the researchers presented a detector model containing these actual parameters, and then evaluated the impact of these problems on actual security. At the same time, aiming at the afterpulse problem, they gave the security random number information upper bound with the existence of eavesdropping.

To solve the problem of detection efficiency mismatch and poor detector sensitivity to the distribution of light source, the researchers proposed a method for monitoring the distribution of light source, and gave a bit rate formula based on the composable security with full consideration to the finite length effect.

This study has quantitatively analyzed the security problem caused by imperfect measurement devices in source-independent quantum random number systems and given the corresponding solutions, which provides an important theoretical support for the realization of ultra-fast commercial source-independent quantum random number generator.

36 Indian IT companies step up fight against cyberattacks

by KAPIL KAJAL

https://asia.nikkei.com/Business/Technology/Indian-IT-companies-step-up-fight-against-cyberattacks?mkt_tok=eyJpIjoiWXpZeE1qY3pOalppTkRWbCIsInQiOiJWNCtcL2tOY2RtNGFwWE9vYTM4c

India's leading IT services companies are ramping up cybersecurity measures to address the increasing threat of cyberattacks across sectors and regions.

Tata Consultancy Services, Infosys, Wipro and HCL Technologies have all started setting up cyber threat management centers mainly in the U.S. and Europe. The largest player TCS had launched 10 centers across the globe that provide cybersecurity services to its enterprise customers by October.

TCS said in a statement that it had opened threat management centers in cities such as Minnesota, Manchester and Madrid, as well as other major Indian cities, in the last four months, with plans to establish "more such centers in other regions."

According to Cybersecurity Ventures, a technology research company, cybercrime in 2021 could lead to damages of up to $6 trillion, a sum bigger than the gross domestic product of Japan, the third-largest economy in the world. In October, India's National Cyber Security Coordinator Rajesh Pant revealed that cybercrime in India caused losses of 1.25 trillion rupees ($17 billion) in 2019.

Traditionally, the largest clients of India's IT industry have been global banks, financial services and insurance companies. As for TCS, these sectors have accounted for 32% of revenue for the quarter ended September. Since cybersecurity is critically important for these clients, the IT industry is rushing to enhance its defense capabilities.

The COVID-19 pandemic has further increased the threat of cyberattacks. According to the Acronis Cyber Readiness Report 2020, during the pandemic, 39% of global companies experienced a videoconferencing attack as workers depend on external apps such as Zoom, Cisco Webex and Microsoft Teams for remote collaboration.

Indian IT companies are also citing the increasing intensity of cyberattacks as well as the need to secure larger areas including remote workplaces amid the pandemic, as reasons for strengthening their countermeasures.

HCL opened its Cybersecurity Fusion Center in Gothenburg, Sweden, its first in Europe in August. The company said that the rapid shift to remote working for many organizations has led to the emergence of new threats, forcing companies to rewrite their security playbooks.

Vijayashankar Nagarajarao, executive chairman at the Foundation of Data Protection Professionals in India, pointed out that the pandemic has increased hacking opportunities because there is greater use of technology by people who may be new to online services, for example, those who were forced by pandemic-induced lockdowns to use online banking services.

“In industries, work from home has also introduced a new threat, and companies who have not been thinking about security faced the music. So that is a reason why cybercrime has gone up,” he said.

Infosys set up a Cyber Defense Center in Indianapolis earlier this year. According to Infosys’ cybersecurity report, 83% of executives view cybersecurity as critical, yet 67% are still struggling to have security embedded in their systems.

Experts believe cybersecurity services can be a new growth opportunity for India’s $190 billion IT industry. “It is a welcoming move by Indian companies as security services have always been a possibility,” Vijayashankar said. “If they have got specialization, it is a value-added service.”

37 Switching to Signal? Turn on these settings now for greater privacy and security

by Adrian Kingsley-Hughes

https://www.zdnet.com/article/switching-to-signal-turn-on-these-settings-now-for-greater-privacy-and-security/

Many people are making the switch from WhatsApp to Signal. Many are switching because of the increased privacy and security that Signal offers.

But with a few simple tweaks, did you know that you can make Signal even more secure?

There are a few settings I suggest you enable. There are some cosmetic differences between the iOS and Android versions of Signal, but these tips apply to both platforms.

The first place you should head over to is the Settings screen. To get there, tap on your initials in the top-left corner of the screen (on Android you can also tap the three dots on the top-left and then Settings).

There are three settings on iOS and four on Android I recommend turning on, and a few others worth taking a look at.

- **Screen Lock (iOS and Android):** Means you have to enter your biometrics (Face ID, Touch ID, fingerprint or passcode) to access the app
- **Enable Screen Security (iOS) or Screen Security (Android):** On the iPhone this prevents data previews being shown in the app switcher, while on Android it prevents screenshots being taken
- **Registration Lock (iOS and Android):** Requires your PIN when registering with Signal (a handy way to prevent a second device being added)

- **Incognito Keyboard (Android only):** Prevents the keyboard from sending what you type to a third-party, which might allow sensitive data to leak

While you're here, Always Relay Calls, a feature which takes all your calls through a Signal server, thus hiding your IP address from the recipient, might be worth enabling, but it does degrade call quality.

On top of this, I suggest that you tame notifications, especially if you are worried about shoulder surfers seeing your messages.

To do this, head back to the main Settings screen and go to Notifications. For Show, change to No Name or Content for iOS and No name or message for Android.

The iOS version of Signal also has a feature called Censorship Circumvention under Advanced, which is handy if you live in an area where there is active internet censorship happening which blocks Signal. If this does not apply to you, leave this off.

38 Important Milestone in the Creation of a Quantum Computer That Uses Transistors As Qubits

by UNIVERSITY OF COPENHAGEN

https://scitechdaily.com/important-milestone-in-the-creation-of-a-quantum-computer-that-uses-transistors-as-qubits/

One of the obstacles for progress in the quest for a working quantum computer has been that the working devices that go into a quantum computer and perform the actual calculations, the qubits, have hitherto been made by universities and in small numbers. But in recent years, a pan-European collaboration, in partnership with French microelectronics leader CEA-Leti, has been exploring everyday transistors – that are present in billions in all our mobile phones – for their use as qubits.

The French company Leti makes giant wafers full of devices, and, after measuring, researchers at the Niels Bohr Institute, University of Copenhagen, have found these industrially produced devices to be suitable as a qubit platform capable of moving to the second dimension, a significant step for a working quantum computer. The result is now published in Nature Communications.

Quantum dots in two dimensional array is a leap ahead

One of the key features of the devices is the two-dimensional array of quantum dot. Or more precisely, a two by two lattice of quantum dots. "What we have shown is that we can realize single electron control in every single one of these quantum dots. This is very important for the development of a qubit, because one of the possible ways of making qubits is to use the spin of a single electron. So reaching this goal of controlling the single electrons and doing it in a 2D array of quantum dots was very important for us," says Fabio Ansaloni, former PhD student, now postdoc at center for Quantum Devices, NBI.

Using electron spins has proven to be advantageous for the implementation of qubits. In fact, their "quiet" nature makes spins weakly interacting with the noisy environment, an important requirement to obtain highly performing qubits.

Extending quantum computers processors to the second dimension has been proven to be essential for a more efficient implementation of quantum error correction routines. Quantum error correction will enable future quantum computers to be fault tolerant against individual qubit failures during the computations.

The importance of industry scale production

Assistant Professor at Center for Quantum Devices, NBI, Anasua Chatterjee adds: “The original idea was to make an array of spin qubits, get down to single electrons and become able to control them and move them around. In that sense it is really great that Leti was able to deliver the samples we have used, which in turn made it possible for us to attain this result. A lot of credit goes to the pan-European project consortium, and generous funding from the EU, helping us to slowly move from the level of a single quantum dot with a single electron to having two electrons, and now moving on to the two dimensional arrays. Two dimensional arrays is a really big goal, because that’s beginning to look like something you absolutely need to build a quantum computer. So Leti has been involved with a series of projects over the years, which have all contributed to this result.”

The credit for getting this far belongs to many projects across Europe

The development has been gradual. In 2015, researchers in Grenoble succeeded in making the first spin qubit, but this was based on holes, not electrons. Back then, the performance of the devices made in the “hole regime” were not optimal, and the technology has advanced so that the devices now at NBI can have two dimensional arrays in the single electron regime. The progress is threefold, the researchers explain: “First, producing the devices in an industrial foundry is a necessity. The scalability of a modern, industrial process is essential as we start to make bigger arrays, for example for small quantum simulators. Second, when making a quantum computer, you need an array in two dimensions, and you need a way of connecting the external world to each qubit. If you have 4-5 connections for each qubit, you quickly end up with a unrealistic number of wires going out of the low-temperature setup. But what we have managed to show is that we can have one gate per electron, and you can read and control with the same gate. And lastly, using these tools we were able to move and swap single electrons in a controlled way around the array, a challenge in itself.”

Two dimensional arrays can control errors

Controlling errors occurring in the devices is a chapter in itself. The computers we use today produce plenty of errors, but they are corrected through what is called the repetition code. In a conventional computer, you can have information in either a 0 or a 1. In order to be sure that the outcome of a calculation is correct, the computer repeats the calculation and if one transistor makes an error, it is corrected through simple majority. If the majority of the calculations performed in other transistors point to 1 and not 0, then 1 is chosen as the result. This is not possible in a quantum computer since you cannot make an exact copy of a qubit, so quantum error correction works in another way: State-of-the-art physical qubits do not have low error rate yet, but if enough of them are combined in the 2D array, they can keep each other in check, so to speak. This is another advantage of the now realized 2D array.

The next step from this milestone

The result realized at the Niels Bohr Institute shows that it is now possible to control single electrons, and perform the experiment in the absence of a magnetic field. So the next step will be to look for spins – spin signatures – in the presence of a magnetic field. This will be essential to implement single and two qubit gates between the single qubits in the array. Theory has shown that a handful of single and two qubit gates, called a complete set of quantum gates, are enough to enable universal quantum computation.

13 Jan 2021

39 Lightweight Crypto, Heavyweight Protection

by Meltem Sonmez Turan

https://www.nist.gov/blogs/taking-measure/lightweight-crypto-heavyweight-protection

Logic puzzles, brain teasers and mathematical riddles fascinated me throughout my childhood, so I feel lucky that I ended up with a career that never lacks for mathematical challenges. Part of my job at the National Institute of Standards and Technology (NIST) involves reviewing the cryptographic algorithms developed to protect our information and identifying possible weaknesses that make them less secure. Searching for these weaknesses reminds me of the process of solving hard mathematical riddles. Although it can sometimes be frustrating, I find it very rewarding.

Over the last couple of years, my focus has been on cryptographic algorithms that are designed to increase the security of small devices like embedded microcontrollers, radio-frequency identification (RFID) tags or sensors. These now ubiquitous devices, found in home automation, smart city technologies, digital assistants and health-care applications, are constrained in terms of their processing power and storage capabilities. Since these devices usually collect, store and process so much important information, users are concerned about their privacy and security. Moreover, due to the lack of suitable cryptographic solutions that perform well in these devices, most of these products do not offer sufficient protection or use proprietary, nonstandard security algorithms that can be reverse-engineered and broken in practice.

New Cryptographic Algorithms Needed

Over the last decade there has been significant research on designing new encryption algorithms optimized for constrained devices. These algorithms are commonly referred to as “lightweight” cryptography algorithms. “Lightweight” does not mean that the algorithms are not secure, but rather that they are efficient to implement and perform well in constrained devices. When we think about the weight of an algorithm, we look at the properties of its implementation in hardware or software. For hardware implementations where the encryption is hardwired into the device, the properties are the physical area needed for a circuit to implement the algorithm, the amount of time it takes to obtain the circuit’s output, and the amount of power needed. For software implementations, the properties are the amount of memory used during evaluation of the algorithm, the size of the compiled code, and the amount of input processed per time unit.

The target metrics and the optimal tradeoff between performance, cost and security usually depend on the technology and applications. In anti-counterfeiting applications, RFID tags with a small amount of memory are commonly used to identify and track retail products. Here, hardware-oriented algorithms that can be implemented in a small area are desired. In smart home appliances with low-end processing units, software-oriented algorithms that consume a small amount of memory are preferred.

After analyzing the performance of current NIST standards on constrained devices, the institute’s Cryptographic Technology Group (CTG) has decided that there is indeed a need for a new lightweight cryptography standard that simultaneously protects the confidentiality and proves the authenticity of the message. To select the new lightweight cryptography standard, CTG decided to organize an international cryptographic competition.

Cryptography Competitions

International cryptography competitions provide an open and transparent process to standardize algorithms. The competitions, especially the ones organized by NIST, are highly visible and bring the cryptography research community, industry stakeholders and other standards-developing organizations together to evaluate and select widely accepted, state-of-the-art algorithms. Cryptographic competitions also attract many graduate students searching for interesting research problems to work on. Due to this interest, the competitions are believed to help the research community gain broader understanding of the field, as numerous research papers and even Ph.D. theses are published as the result of the process.

In 1997, NIST initiated a public competition to develop a replacement for the Data Encryption Standard, which was initially adopted in 1977, and received 15 international submissions. In 2000, the submission Rijndael, designed by Joan Daemen and Vincent Rijmen, was selected as the winner of the competition and dubbed the Advanced Encryption Standard (AES). According to a study commissioned by NIST, the economic impact of the development of AES has been more than $250 billion since its selection. In 2007, NIST announced another competition to select a new hash function standard named SHA-3. This competition received 64 submissions, and in 2012, NIST selected Keccak as the new hash function standard.

Setting the Standard for Lightweight Cryptography

In 2018, NIST announced the lightweight cryptography competition to solicit, evaluate and standardize algorithms that are suitable for constrained environments. The announcement in the Federal Register specified the technical requirements for the target cryptographic algorithm and explained the evaluation criteria and a tentative timeline.

The competition received 57 submission packages from 25 different countries, where each package included algorithm specifications, intellectual property statements and portable reference software implementations. We were happy and surprised to receive such a large number of submissions. Similar to other competitions, we planned for having multiple rounds, where in each round the field is narrowed to focus on the most promising candidates. We advanced 32 of these candidates to the second round based on their security properties. As the next step, we plan to select around eight finalists that perform significantly better than current NIST standards in software and hardware. After one more year of extensive analysis and performance benchmarking, we plan to select the winner and add a new crypto standard to NIST's portfolio.

Although being in the review committee of these competitions is challenging, it also provides an amazing opportunity to learn and exchange new ideas, work as a team with the cryptographic research community with the goal of selecting a secure algorithm. I look forward to working on more of these mathematical challenges and helping to improve cryptographic standards in the future.

40 Google to use quantum computing to develop new medicines

by Aditya Saroha

https://www.thehindu.com/sci-tech/technology/google-to-use-quantum-computing-to-develop-new-medicines/article33564897.ece

Google's Quantum AI division has partnered with German pharmaceutical company, Boehringer Ingelheim, to develop new drugs using quantum computing.

Through this collaboration, Boehringer Ingelheim and Google plan to focus on implementing quantum computing in pharmaceutical research and development, including molecular dynamic simulations.

While Boehringer Ingelheim will focus on computer-aided drug design and in silico modelling, Google will supply quantum computers and algorithms.

“Together with Google, our goal is to apply the use of quantum computing in biopharmaceutical R&D and thus continue to make a decisive contribution to medical progress for patients around the world,” Michel Pairet, Board member responsible for the company’s Innovation Unit at Boehringer Ingelheim, said in a statement.

The idea is to use quantum computing to solve complex challenges during the early stages of pharmaceutical R&D, which today’s computers are unable to resolve.

According to Boehringer Ingelheim, Quantum computing has the potential to accurately simulate and compare much larger molecules than currently possible. This will create new opportunities for pharmaceutical innovation and therapies for a range of diseases.

“Extremely accurate modelling of molecular systems is widely anticipated as among the most natural and potentially transformative applications of quantum computing,” Ryan Babbush, Head of Quantum Algorithms at Google said.

Boehringer Ingelheim said it is the first pharmaceutical company worldwide to join forces with Google in quantum computing. The partnership is designed for three years and is co-led by the newly established Quantum Lab of Boehringer Ingelheim.

41 China Builds the World’s First Integrated Quantum Communication Network

by UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA

https://scitechdaily.com/china-builds-the-worlds-first-integrated-quantum-communication-network/

Chinese scientists have established the world’s first integrated quantum communication network, combining over 700 optical fibers on the ground with two ground-to-satellite links to achieve quantum key distribution over a total distance of 4,600 kilometers for users across the country. The team, led by Jianwei Pan, Yuao Chen, Chengzhi Peng from the University of Science and Technology of China in Hefei, reported in Nature their latest advances towards the global, practical application of such a network for future communications.

Unlike conventional encryption, quantum communication is considered unhackable and therefore the future of secure information transfer for banks, power grids and other sectors. The core of quantum communication is quantum key distribution (QKD), which uses the quantum states of particles – e.g. photons – to form a string of zeros and ones, while any eavesdropping between the sender and the receiver will change this string or key and be noticed immediately. So far, the most common QKD technology uses optical fibers for transmissions over several hundred kilometers, with high stability but considerable channel loss. Another major QKD technology uses the free space between satellites and ground stations for thousand-kilometer-level transmissions. In 2016, China launched the world’s first quantum communication satellite (QUESS, or Mozi/Micius) and achieved QKD with two ground stations which are 2,600 km apart. In 2017, an over 2,000-km-long optical fiber network was completed for QKD between Beijing and Shanghai.

Using trusted relays, the ground-based fiber network and the satellite-to-ground links were integrated to serve more than 150 industrial users across China, including state and local banks, municipal power grids, and e-government websites. "Our work shows that quantum communication technology is sufficiently mature for large-scale practical applications," said Jianwei Pan, Professor of USTC. Similarly, a global quantum communication network can be established if national quantum networks from different countries are combined, and if universities, institutions and companies come together to standardize related protocols, hardware, etc., he added.

In the last couple of years, the team extensively tested and improved the performance of different parts of the integrated network. For instance, with an increased clock rate and more efficient QKD protocol, the satellite-to-ground QKD now has an average key generation rate of 47.8 kilobits per second, which is 40 times higher than the previous rate. The researchers have also pushed the record for ground-based QKD to beyond 500 km using a new technology called **twin-field QKD (TF-QKD)**.

Next up, the team will further expand the network in China and with their international partners from Austria, Italy, Russia and Canada. They also aim to develop small-scale, cost-efficient QKD satellites and ground-based receivers, as well as medium and high earth orbit satellites to achieve all-time, ten-thousand-km-level QKD.

11 Jan 2021

42 Electrically switchable qubit can tune between storage and fast calculation modes

https://www.unibas.ch/en/News-Events/News/Uni-Research/Electrically-switchable-qubit-can-tune-between-storage-and-fast-calculation-modes.html

To perform calculations, quantum computers need qubits to act as elementary building blocks that process and store information. Now, physicists have produced a new type of qubit that can be switched from a stable idle mode to a fast calculation mode. The concept would also allow a large number of qubits to be combined into a powerful quantum computer, as researchers from the University of Basel and TU Eindhoven have reported in the journal "Nature Nanotechnology".

Compared with conventional bits, quantum bits (qubits) are much more fragile and can lose their information content very quickly. The challenge for quantum computing is therefore to keep the sensitive qubits stable over a prolonged period of time, while at the same time finding ways to perform rapid quantum operations. Now, physicists from the University of Basel and TU Eindhoven have developed a switchable qubit that should allow quantum computers to do both.

The new type of qubit has a stable but slow state that is suitable for storing quantum information. However, the researchers were also able to switch the qubit into a much faster but less stable manipulation mode by applying an electrical voltage. In this state, the qubits can be used to process information quickly.

Selective coupling of individual spins

In their experiment, the researchers created the qubits in the form of "hole spins". These are formed when an electron is deliberately removed from a semiconductor, and the resulting hole has a spin that can adopt two states, up and down – analogous to the values 0 and 1 in classical bits. In the new type of qubit, these spins can be selectively coupled – via a photon, for example – to other spins by tuning their resonant frequencies.

This capability is vital, since the construction of a powerful quantum computer requires the ability to selectively control and interconnect many individual qubits. Scalability is particularly necessary to reduce the error rate in quantum calculations.

Ultrafast spin manipulation

The researchers were also able to use the electrical switch to manipulate the spin qubits at record speed. “The spin can be coherently flipped from up to down in as little as a nanosecond,” says project leader Professor Dominik Zumbühl from the Department of Physics at the University of Basel. “That would allow up to a billion switches per second. Spin qubit technology is therefore already approaching the clock speeds of today’s conventional computers.”

For their experiments, the researchers used a semiconductor nanowire made of silicon and germanium. Produced at TU Eindhoven, the wire has a tiny diameter of about 20 nanometers. As the qubit is therefore also extremely small, it should in principle be possible to incorporate millions or even billions of these qubits onto a chip.

08 Jan 2021

43 Researchers realize efficient generation of high-dimensional quantum teleportation

by University of Science and Technology of China

https://phys.org/news/2021-01-efficient-high-dimensional-quantum-teleportation.html

In a study published in Physical Review Letters, a team led by academician Guo Guangcan from the University of Science and Technology of China (USTC) of the Chinese Academy of Sciences (CAS) has made progress in high dimensional quantum teleportation. The researchers demonstrated the teleportation of high-dimensional states in a three-dimensional six-photon system.

To transmit unknown quantum states from one location to another, quantum teleportation is one of the key technologies to realize long-distance transmission.

Compared with two-dimensional systems, high-dimensional system quantum networks have the advantages of higher channel capacity and better security. In recent years more and more researchers of the quantum information field have been working on generating efficient generation of high-dimensional quantum teleportation to achieve efficient high-dimensional quantum networks.

As early as 2016, the researchers from USTC experimentally showed that nonlocality can be produced from single-particle contextuality through two-particle correlations which do not violate any Bell inequality by themselves, and generated high-fidelity three-dimensional entanglement. In 2020, 32-dimensional quantum entanglement and efficient distribution of high-dimensional entanglement through 11 km fiber were respectively achieved to lay a solid foundation for scalable quantum networks.

In a linear optical system, auxiliary entanglement is the key to realizing high-dimensional quantum teleportation. The researchers exploited the spatial mode (path) to encode the three-dimensional states that has been demonstrated to extremely high-fidelity, and used an auxiliary entangled photon pair to perform the high-dimensional Bell state measurement (HDBSM), demonstrating the teleportation of a three-dimensional quantum state using the spatial mode of a single photon.

In this work, the fidelity of teleportation process matrix could reach 0.5967, which is seven standard deviations above the fidelity of 1/3, which proves the teleportation is both non-classical and genuinely three dimensional.

This study paves the way to rebuild complex quantum systems remotely and to construct complex quantum networks. It will promote the research on high-dimensional quantum information tasks. Entanglement-assisted methods for HDBSM are feasible for other high-dimensional quantum information tasks.

44 Hackers can clone Google Titan 2FA keys using a side channel in NXP chips

by DAN GOODIN

https://arstechnica.com/information-technology/2021/01/hackers-can-clone-google-titan-2fa-keys-using-a-side-channel-in-nxp-chips/

There's wide consensus among security experts that physical two-factor authentication keys provide the most effective protection against account takeovers. Research published today doesn't change that thinking, but it does show how malicious attackers with physical possession of a Google Titan key can clone it.

There are some steep hurdles to clear for an attack to be successful. A hacker would first have to steal a target's account password and also gain covert possession of the physical key for as many as 10 hours. The cloning also requires up to $12,000 worth of equipment and custom software, plus an advanced background in electrical engineering and cryptography. That means the key cloning – were it ever to happen in the wild – would likely be done only by a nation-state pursuing its highest-value targets.

"Nevertheless, this work shows that the Google Titan Security Key (or other impacted products) would not avoid [an] unnoticed security breach by attackers willing to put enough effort into it," researchers from security firm NinjaLab wrote in a research paper published Thursday. "Users that face such a threat should probably switch to other FIDO U2F hardware security keys, where no vulnerability has yet been discovered."

The 2FA gold standard

Two-factor authentication, or 2FA, is a method that makes account takeovers much harder to pull off. Instead of using only a password to prove someone is authorized to access an account, 2FA requires a second factor, such as a one-time password, possession of a physical object, or a fingerprint or other biometric.

Physical keys are among the – if not the – most secure forms of 2FA because they store the long-term secret that makes them work internally, and only output non-reusable values. The secret is also impossible to phish. Physical keys are also more convenient, since they work on all major operating systems and hardware. The Titan vulnerability is one of the only weaknesses ever to be found in a mainstream 2FA key. However improbable, a successful real-world exploit would completely undermine the security assurances the thumb-size devices provide. The NinjaLab researchers are quick to point out that despite the weakness, it's still safer to use a Titan Security Key or another affected authentication device to sign in to accounts than not to.

Attack of the clones

The cloning works by using a hot air gun and a scalpel to remove the plastic key casing and expose the NXP A700X chip, which acts as a secure element that stores the cryptographic secrets. Next, an attacker connects the chip to hardware and software that take measurements as the key is being used to authenticate on an existing account. Once the measurement-taking is finished, the attacker seals the chip in a new casing and returns it to the victim.

Extracting and later resealing the chip takes about four hours. It takes another six hours to take measurements for each account the attacker wants to hack. In other words, the process would take 10 hours to clone the key for a single account, 16 hours to clone a key for two accounts, and 22 hours for three accounts.

By observing the local electromagnetic radiations as the chip generates the digital signatures, the researchers exploit a side channel vulnerability in the NXP chip. The exploit allows an attacker to obtain the long-term elliptic curve digital signal algorithm private key designated for a given account. With the crypto key in hand, the attacker can then create her own key, which will work for each account she targeted.

Paul Kocher, an independent cryptography expert with no involvement in the research, said that while the real-world risk of the attack is low, the side-channel discovery is nonetheless important, given the class of users – dissidents, lawyers, journalists, and other high-value targets – who rely on it and the possibility that attacks will improve over time.

“The work is notable because it’s a successful attack against a well-hardened target designed for high-security applications, and clearly breaks the product’s security characteristics,” he wrote in an email. “A real adversary might well be able to refine the attack (e.g., shortening the data collection time and/or removing the need to physically open the device). For example, the attack might be extendable to a token left in a hotel gym locker for an hour.”

Doing the impossible

Indeed, the Google Titan, like other security keys that use the FIDO U2F standard, is supposed to make it impossible to transfer crypto keys and signatures off the device, as the NinjaLab researchers noted:

> As we have seen, the FIDO U2F protocol is very simple, the only way to interact with the U2F device is by registration or authentication requests. The registration phase will generate a new ECDSA key pair and output the public key. The authentication will mainly execute an ECDSA signature operation where we can choose the input message and get the output signature.
>
> Hence, even for a legitimate user, there is no way to know the ECDSA secret key of a given application account. This is a limitation of the protocol which, for instance, makes [it] impossible to transfer the user credentials from one security key to another. If a user wants to switch to a new hardware security key, a new registration phase must be done for every application account. This will create new ECDSA key pairs and revoke the old ones.
>
> This limitation in functionality is a strength from a security point-of-view: by design it is not possible to create a clone. It is moreover an obstacle for side-channel reverse-engineering. With no control whatsoever on the secret key it is barely possible to understand the details of (let alone to attack) a highly secured implementation. We will have to find a workaround to study the implementation security in a more convenient setting.

Risk assessment

Despite describing a way to compromise the security of a key Google sells, the research won't receive a payment under Google's bug bounty program, which provides rewards to hackers who discover security flaws in Google products or services and privately report them to the company. A Google spokeswoman said that attacks that require physical possession are out of scope of the company's security key threat model. She also noted the difficulty and expense in carrying out an attack.

While the researchers performed their attack on the Google Titan, they believe that other hardware that uses the A700X, or chips based on the A700X, may also be vulnerable. If true, that would include Yubico's YubiKey NEO and several 2FA keys made by Feitian.

In an email, Yubico spokeswoman Ashton Miller said the company is aware of the research and believes its findings are accurate. "While the researchers note that physical device access, expensive equipment, custom software, and technical skills are required for this type of attack, Yubico recommends revoking access for a lost, stolen, or misplaced YubiKey NEO to mitigate risk," she wrote.

In a statement, NXP officials wrote:

> NXP is aware of the report and appreciates the co-operation of the researchers. Since October 2020 we have actively communicated to the majority of potentially affected customers and given them the opportunity to discuss with our security experts. This effort is almost completed. We encourage customers to complete their own risk assessment for their systems and applications that use the affected products. The root cause cannot be fixed in the affected products. However, there are use-cases where countermeasures may be applied on system level. Newer generations of these products with additional countermeasures are available.

Representatives from Feitian weren't immediately available for comment.

One countermeasure that can partially mitigate the attack is for service providers that offer key-based 2FA to use a feature baked into the U2F standard that counts the number of interactions a key has had with the provider's servers. If a key reports a number that doesn't match what's stored on the server, the provider will have good reason to believe the key is a clone. A Google spokeswoman said the company has this feature.

The research – from Ninjalab co-founders Victor Lomné and Thomas Roche in Montpellier, France – is impressive, and in time, it's likely to result in the side-channel vulnerability being fixed. In the meantime, the vast majority of people using an affected key should continue doing so, or at the very most, switch to a key with no known vulnerabilities. The worst outcome from this research would be for people to stop using physical security keys altogether.

45 Cryptography Research Centre in Abu Dhabi and Yale University to research post-quantum cryptography

https://www.helpnetsecurity.com/2021/01/08/technology-innovation-institutes-cryptography-research-centre-yale/

Abu Dhabi and the UAE are working to pioneer breakthroughs in post-quantum cryptography and neuromorphic computing through an international partnership between Technology Innovation Institute's

(TII) Cryptography Research Centre (CRC) and Yale University, an Ivy League research university in Connecticut, United States.

The two institutions will first join forces on 'Post-Quantum Lightweight Crypto Hardware Accelerators and Trusted Execution Environment Designs', a project at the intersection of emerging technologies that focuses on developing quantum-resistant crypto schemes within the context of emerging quantum algorithms that can be run on a sufficiently large quantum computer.

By leveraging post-quantum cryptographic (PQC) algorithms, the project aims to guarantee the necessary measures of security even as today's public cryptographic standards, such as RSA and Elliptic Curve Cryptography (ECC), become ineffective when a powerful quantum computer is built and can run Shor's quantum algorithm. The project is also exploring post-quantum lightweight cryptography with a focus on highly constrained devices.

The neuromorphic computing project, 'Energy-based Probing for Robust and Explainable Spiking Neural Networks', takes inspiration from the brain to create energy-efficient hardware for information processing and is capable of highly sophisticated tasks.

The project examines Spiking Neural Networks (SNNs), which have become popular as an energy-efficient alternative for implementing standard artificial intelligence tasks. Spikes or binary events drive communication and computation in SNNs that are close to biological neuronal processing and offer the benefit of event-driven hardware operations.

The central focus of the collaboration is to explore the design space of the energy-accuracy-robustness-explainability trade-off and to design the hardware/software necessary to create truly functional intelligent systems. To ensure there is no overlap, both entities have been tasked with managing specific areas of the research in both projects.

Speaking on the partnership, Dr Najwa Aaraj, Chief Researcher at Cryptography Research Centre, said: "We are excited to work with peers from Yale University in carrying out groundbreaking research in these two vital fields. At the Cryptography Research Centre, we are creating a knowledge-driven ecosystem powered by like-minded scientists and researchers – all focused on designing breakthrough solutions in different areas of cryptography."

Jakub Szefer, Associate Professor of Electrical Engineering and Computer Science, and Priya Panda, Assistant Professor of Electrical Engineering, from Yale University, said: "By working collaboratively with Cryptography Research Centre, we have an opportunity to apply shared expertise across post-quantum cryptography and neuromorphic computing research. We are optimistic that this partnership will yield effective research outcomes for greater impact."

Technology Innovation Institute, the 'applied research' pillar of Advanced Technology Research Council (ATRC), is a pioneering global research and development centre that focuses on applied research and new-age technology capabilities.

The institute has seven initial dedicated research centres in quantum, autonomous robotics, cryptography, advanced materials, digital security, directed energy and secure systems.

By working with exceptional talent, universities, research institutions and industry partners from all over the world, the Institute connects an intellectual community and contributes to building an R&D ecosystem in Abu Dhabi and the UAE.

The Institute reinforces Abu Dhabi and the UAE's status as a global hub for innovation and contributes to the broader development of the knowledge- based economy.

46 Hidden Symmetry Could Be Key to Ultra-Powerful Quantum Computers

by University of Cambridge

https://scitechdaily.com/hidden-symmetry-could-be-key-to-ultra-powerful-quantum-computers/amp/

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

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

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

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

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

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

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

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

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

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

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

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

07 Jan 2021

47 Research team demonstrates world’s fastest optical neuromorphic processor

by Swinburne University of Technology

https://techxplore.com/news/2021-01-team-world-fastest-optical-neuromorphic.html

An international team of researchers led by Swinburne University of Technology has demonstrated the world’s fastest and most powerful optical neuromorphic processor for artificial intelligence (AI), which operates faster than 10 trillion operations per second (TeraOPs/s) and is capable of processing ultra-large scale data. Published in the prestigious journal Nature, this breakthrough represents an enormous leap forward for neural networks and neuromorphic processing in general.

Artificial neural networks, a key form of AI, can ‘learn’ and perform complex operations with wide applications to computer vision, natural language processing, facial recognition, speech translation, playing strategy games, medical diagnosis and many other areas. Inspired by the biological structure of the brain’s visual cortex system, artificial neural networks extract key features of raw data to predict properties and behavior with unprecedented accuracy and simplicity.

Led by Swinburne’s Professor David Moss, Dr. Xingyuan (Mike) Xu (Swinburne, Monash University) and Distinguished Professor Arnan Mitchell from RMIT University, the team achieved an exceptional feat in optical neural networks: dramatically accelerating their computing speed and processing power.

The team demonstrated an optical neuromorphic processor operating more than 1000 times faster than any previous processor, with the system also processing record-sized ultra-large scale images – enough to achieve full facial image recognition, something that other optical processors have been unable to accomplish.

“This breakthrough was achieved with ‘optical micro-combs,” as was our world-record internet data speed reported in May 2020,” says Professor Moss, Director of Swinburne’s Optical Sciences Centre.

While state-of-the-art electronic processors such as the Google TPU can operate beyond 100 TeraOPs/s, this is done with tens of thousands of parallel processors. In contrast, the optical system demonstrated by the team uses a single processor and was achieved using a new technique of simultaneously interleaving the data in time, wavelength and spatial dimensions through an integrated micro-comb source.

Micro-combs are relatively new devices that act like a rainbow made up of hundreds of high-quality infrared lasers on a single chip. They are much faster, smaller, lighter and cheaper than any other optical source.

“In the 10 years since I co-invented them, integrated micro-comb chips have become enormously important and it is truly exciting to see them enabling these huge advances in information communication and processing. Micro-combs offer enormous promise for us to meet the world’s insatiable need for information,” says Professor Moss.

“This processor can serve as a universal ultrahigh bandwidth front end for any neuromorphic hardware – optical or electronic based– bringing massive-data machine learning for real-time ultrahigh bandwidth data within reach,” says co-lead author of the study, Dr. Xu, Swinburne alum and postdoctoral fellow with the Electrical and Computer Systems Engineering Department at Monash University.

“We’re currently getting a sneak-peak of how the processors of the future will look. It’s really showing us how dramatically we can scale the power of our processors through the innovative use of microcombs,” Dr. Xu explains.

RMIT’s Professor Mitchell adds, “This technology is applicable to all forms of processing and communications – it will have a huge impact. Long term we hope to realize fully integrated systems on a chip, greatly reducing cost and energy consumption.”

“Convolutional neural networks have been central to the artificial intelligence revolution, but existing silicon technology increasingly presents a bottleneck in processing speed and energy efficiency,” says key supporter of the research team, Professor Damien Hicks, from Swinburne and the Walter and Elizabeth Hall Institute.

He adds, “This breakthrough shows how a new optical technology makes such networks faster and more efficient and is a profound demonstration of the benefits of cross-disciplinary thinking, in having the inspiration and courage to take an idea from one field and using it to solve a fundamental problem in another.”

48 WhatsApp gives users an ultimatum: Share data with Facebook or stop using the app

by DAN GOODIN

https://arstechnica.com/tech-policy/2021/01/whatsapp-users-must-share-their-data-with-facebook-or-stop-using-the-app/

WhatsApp, the Facebook-owned messenger that claims to have privacy coded into its DNA, is giving its 2 billion plus users an ultimatum: agree to share their personal data with the social network or delete their accounts.

The requirement is being delivered through an in-app alert directing users to agree to sweeping changes in the WhatsApp terms of service. Those who don’t accept the revamped privacy policy by February 8 will no longer be able to use the app.

Share and share alike

Shortly after Facebook acquired WhatsApp for $19 billion in 2014, its developers built state-of-the-art end-to-end encryption into the messaging app. The move was seen as a victory for privacy advocates because it used the Signal Protocol, an open source encryption scheme whose source code has been reviewed and audited by scores of independent security experts.

In 2016, WhatsApp gave users a one-time ability to opt out of having account data turned over to Facebook. Now, an updated privacy policy is changing that. Come next month, users will no longer have that choice. Some of the data that WhatsApp collects includes:

- User phone numbers
- Other people's phone numbers stored in address books
- Profile names
- Profile pictures and
- Status message including when a user was last online
- Diagnostic data collected from app logs

Under the new terms, Facebook reserves the right to share collected data with its family of companies.

"As part of the Facebook family of companies, WhatsApp receives information from, and shares information with, this family of companies," the new privacy policy states. "We may use the information we receive from them, and they may use the information we share with them, to help operate, provide, improve, understand, customize, support, and market our Services and their offerings."

In some cases, such as when someone uses WhatsApp to interact with third-party businesses, Facebook may also share information with those outside entities.

A lack of transparency

The move comes a month after Apple started requiring iOS app makers, including WhatsApp, to detail the information they collect from users. WhatsApp, according to the App Store, reserves the right to collect:

- Purchases
- Financial information
- Location
- Contacts
- User content
- Identifiers
- Usage data and
- Diagnostics

A WhatsApp spokeswoman declined to speak on the record about the changes and precisely how or if it's possible for users to opt out of them. She agreed to email additional information on the condition it be kept on background, meaning none of the details can be quoted verbatim.

The move, the spokeswoman said, is part of a previously disclosed move to allow businesses to store and manage WhatsApp chats using Facebook's infrastructure. Users won't have to use WhatsApp to interact with the businesses and have the option of blocking the businesses. She said there will be no change in how WhatsApp shares provides data with Facebook for non-business chats and account data.

Together, the WhatsApp privacy policy and terms of service are more than 8,000 words long and are filled with legal jargon that makes it difficult for non-lawyers to understand. WhatsApp is doing its users a disservice by not agreeing to speak on the record so that reporters can fully understand the changes and explain them to readers.

People who object to the new terms and policy should consider using a different messenger. The Signal messenger provides the same robust encryption engine with a much more transparent privacy policy and terms of service. (Those documents are half the length of those from WhatsApp, too.) Besides providing encrypted chats, Signal also offers encrypted audio and video calls.

49 Elastic Diamonds could help Quantum Computers run at room temperature

https://www.swissquantumhub.com/elastic-diamonds-could-help-quantum-computers-run-at-room-temperature/

Scientists have found a way to grow diamonds in the lab that can be stressed and strained to give them special electricity-conducting properties.

In addition to being tough, diamonds are highly conductive when it comes to both electricity and heat. Diamond is an extreme electronic material with an ultrawide bandgap, exceptional carrier mobilities, and thermal conductivity. Applying relatively large amounts of strain to diamond may shift its electronic properties, which is of interest for a number of applications.

The team microfabricated single-crystalline diamond bridge structures with ≈1 micrometer length by ≈100 nanometer width and achieved sample-wide uniform elastic strains under uniaxial tensile loading along the [100], [101], and [111] directions at room temperature.

They also demonstrated deep elastic straining of diamond microbridge arrays. The ultralarge, highly controllable elastic strains can fundamentally change the bulk band structures of diamond, including a substantial calculated bandgap reduction as much as ≈2 electron volts.

This demonstration highlights the immense application potential of deep elastic strain engineering for photonics, electronics, and quantum information technologies.

06 Jan 2021

50 The world's first integrated quantum communication network

by University of Science and Technology of China https://phys.org/news/2021-01-world-quantum-network.html

Chinese scientists have established the world's first integrated quantum communication network, combining over 700 optical fibers on the ground with two ground-to-satellite links to achieve quantum key distribution over a total distance of 4,600 kilometers for users across the country. The team, led by Jianwei Pan, Yuao Chen, Chengzhi Peng from the University of Science and Technology of China in Hefei, reported in Nature their latest advances towards the global, practical application of such a network for future communications.

Unlike conventional encryption, quantum communication is considered unhackable and therefore the future of secure information transfer for banks, power grids and other sectors. The core of quantum communication is quantum key distribution (QKD), which uses the quantum states of particles – e.g. photons – to form a string of zeros and ones, while any eavesdropping between the sender and the receiver will change this string or key and be noticed immediately. So far, the most common QKD technology uses optical fibers for transmissions over several hundred kilometers, with high stability but considerable channel loss. Another major QKD technology uses the free space between satellites and ground stations for thousand-kilometer-level transmissions. In 2016, China launched the world's first quantum communication satellite (**QUESS, or Mozi/Micius**) and achieved QKD with two ground stations which are 2,600 km apart. In 2017, an over 2,000-km long optical fiber network was completed for QKD between Beijing and Shanghai.

Using trusted relays, the ground-based fiber network and the satellite-to-ground links were integrated to serve more than 150 industrial users across China, including state and local banks, municipal power grids, and e-government websites. This work shows that quantum communication technology can be used for future large-scale practical applications. Similarly, a global quantum communication network can be established if national quantum networks from different countries are combined, and if universities, institutions and companies come together to standardize related protocols, hardware.

In the last couple of years, the team extensively tested and improved the performance of different parts of the integrated network. For instance, with an increased clock rate and more efficient QKD protocol, the satellite-to-ground QKD now has an average key generation rate of 47.8 kilobits per second, which is 40 times higher than the previous rate. The researchers have also pushed the record for ground-based QKD to beyond 500 km using a new technology called twin-field QKD (TF-QKD).

Next up, the team will further expand the network in China and with their international partners from Austria, Italy, Russia and Canada. They also aim to develop small-scale, cost-efficient QKD satellites and ground-based receivers, as well as medium and high earth orbit satellites to achieve all-time, ten-thousand-km-level QKD.

51 2021 Quantum Predictions and 2020 Predictions Analysis!

https://www.swissquantumhub.com/2021-quantum-predictions-and-2020-predictions-analysis/

It's always amazing in January to sit back and check our previous year predictions with easy criticism and to predict new year facts with a fair dose of optimism. And a bit of humor too.

So here are our quantum 2020 predictions review and our top quantum 2021 predictions. Feel free to comment, we'll appreciate.

By the way, we wish you a very nice Quantum 2021 New Year!

Our quantum 2020 predictions review

In January 2020, we proposed our Top Ten 2020 quantum predictions. Let's review them!

(i) **Intel will announce a quantum breakthrough with silicon qubits** – Hum, though Intel quantum commitment is actually heavy (just check how many Intel guys you can track in university quantum labs worldwide ...) and Horse Ridge cryogenic chip comes to 2nd-Gen, there is no quantum breakthrough still there. **4/10**

(ii) **TU Delft will be the most exciting quantum university** – Rather true. With quantum personalities like Stephanie Wehner, Paul de Wit, and QuTech partnership (Menno Veldhorst), TU Delft is a key player in quantum core technologies and quantum Internet research. **8/10**

(iii) **A financial company (probably US-based) will announce a breakthrough in fast trading and/or portfolio risk assessment using quantum algorithms** – There is no actually breakthrough in this domain but some smart startups in US (Chicago Quantum, Zapata Computing) and in Spain (Multiverse) have collaborated with major banks (Bankia, CaixaBank, BBVA, JPMorgan Chase) to build use cases. **7/10**

(iv) **At least ten startups will get more than $500M each in funding** – Wrong. We have been more than optimistic even though Psiquantum raised big figures. **2/10**

(v) **Israël will be the new quantum startup nation with some surprising startups exiting from shadow mode** – Not too bad. With a $350M public budget over 6 years and VCs like Entrée Capital, Israël is definitely a key player in quantum. A bunch of amazing quantum startups also emerged like Classiq or Quantum Machines. **7/10**

(vi) **Startup consolidation phase will begin with first generation companies buying new ones** – Not exactly true. We didn't see major acquisition but corporate venture branches of big names quantum players (IBM, Fujitsu, Bosch, Honeywell, Google, ...) have invested noticeably in quantum startups. **5/10**

(vii) **Quantum business will mainly be driven by military investments in quantum sensing and QKD security** – Average true. QKD security momentum in China is huge and very probably linked to military concerns (and funding). Quantum sensing its currently more related to medical and scientific devices. But military quantum lobbying has been dramatically intense in USA. Quantum radar prototypes have been tested in major countries. **6/10**

(viii) **IBM will announce new quantum volume achievement** – True! **10/10**

(ix) **Google will achieve new quantum supremacy** – False! **0/10**

2021 Top Quantum Predictions

Here are our Top Ten 2021 quantum predictions. See you in 2022 to check them!

1. Intel will announce a quantum breakthrough with silicon qubits (yes, we still strongly believe that!)
2. Quantum technologies, especially QKD and quantum sensing, will become a key issue in international relationships, space treaties, export regulations, and USA-China economy and soft-power war.

3. There will be a major quantum company IPO (Rigetti?)

4. Startup consolidation phase will begin with acquisitions (2020 prediction ...)

5. QRNGs (Quantum Random Number Generators) will be widely used by several industries (5G, gaming, casinos, finance)

6. France will at least introduce a quantum plan and will fund it with actual money (friendly message to all the smart French quantum startups: guys, keep on the good job and hope!)

7. Swiss banks will at least understand medium-term impact of quantum computing to their operations and urge to build business cases with the help of Swiss universities (private joke)

05 Jan 2021

52 New Quantum Algorithms Finally Crack Nonlinear Equations

by Max G. Levy

https://www.quantamagazine.org/new-quantum-algorithms-finally-crack-nonlinear-equations-20210105/

Sometimes, it's easy for a computer to predict the future. Simple phenomena, such as how sap flows down a tree trunk, are straightforward and can be captured in a few lines of code using what mathematicians call linear differential equations. But in nonlinear systems, interactions can affect themselves: When air streams past a jet's wings, the air flow alters molecular interactions, which alter the air flow, and so on. This feedback loop breeds chaos, where small changes in initial conditions lead to wildly different behavior later, making predictions nearly impossible – no matter how powerful the computer.

"This is part of why it's difficult to predict the weather or understand complicated fluid flow," said Andrew Childs, a quantum information researcher at the University of Maryland. "There are hard computational problems that you could solve, if you could [figure out] these nonlinear dynamics."

That may soon be possible. In separate studies posted in November, two teams – one led by Childs, the other based at the Massachusetts Institute of Technology – described powerful tools that would allow quantum computers to better model nonlinear dynamics.

Quantum computers take advantage of quantum phenomena to perform certain calculations more efficiently than their classical counterparts. Thanks to these abilities, they can already topple complex linear differential equations exponentially faster than classical machines. Researchers have long hoped they could similarly tame nonlinear problems with clever quantum algorithms.

The new approaches disguise that nonlinearity as a more digestible set of linear approximations, though their exact methods vary considerably. As a result, researchers now have two separate ways of approaching nonlinear problems with quantum computers.

"What is interesting about these two papers is that they found a regime where, given some assumptions, they have an algorithm that is efficient," said Mária Kieferová, a quantum computing researcher at the University of Technology Sydney who is not affiliated with either study. "This is really exciting, and [both studies] use really nice techniques."

The Cost of Chaos

Quantum information researchers have tried to use linear equations as a key to unlock nonlinear differential ones for over a decade. One breakthrough came in 2010, when Dominic Berry, now at Macquarie University in Sydney, built the first algorithm for solving linear differential equations exponentially faster on quantum, rather than on classical, computers. Soon, Berry's own focus shifted to nonlinear differential equations as well.

"We had done some work on that before," Berry said. "But it was very, very inefficient."

The problem is, the physics underlying quantum computers is itself fundamentally linear. "It's like teaching a car to fly," said Bobak Kiani, a co-author of the MIT study.

So the trick is finding a way to mathematically convert a nonlinear system into a linear one. "We want to have some linear system because that's what our toolbox has in it," Childs said. The groups did this in two different ways.

Childs' team used Carleman linearization, an out-of-fashion mathematical technique from the 1930s, to transform nonlinear problems into an array of linear equations.

Unfortunately, that list of equations is infinite. Researchers have to figure where they can cut off the list to get a good-enough approximation. "Do I stop at equation number 10? Number 20?" said Nuno Loureiro, a plasma physicist at MIT and a co-author of the Maryland study. The team proved that for a particular range of nonlinearity, their method could truncate that infinite list and solve the equations.

The MIT-led paper took a different approach. It modeled any nonlinear problem as a Bose-Einstein condensate. This is a state of matter where interactions within an ultracold group of particles cause each individual particle to behave identically. Since the particles are all interconnected, each particle's behavior influences the rest, feeding back to that particle in a loop characteristic of nonlinearity.

The MIT algorithm mimics this nonlinear phenomenon on a quantum computer, using Bose-Einstein math to connect nonlinearity and linearity. So by imagining a pseudo Bose-Einstein condensate tailor made for each nonlinear problem, this algorithm deduces a useful linear approximation. "Give me your favorite nonlinear differential equation, then I'll build you a Bose-Einstein condensate that will simulate it," said Tobias Osborne, a quantum information scientist at Leibniz University Hannover who was not involved in either study. "This is an idea I really loved."

Berry thinks both papers are important in different ways (he wasn't involved with either). "But ultimately the importance of them is showing that it's possible to take advantage of [these methods] to get the nonlinear behavior," he said.

Knowing One's Limits

While these are significant steps, they are still among the first in cracking nonlinear systems. More researchers will likely analyze and refine each method – even before the hardware needed to implement them becomes a reality. "With both of these algorithms, we are really looking in the future," Kieferová said. Using them to solve practical nonlinear problems requires quantum computers with thousands of qubits to minimize error and noise – far beyond what's possible today.

And both algorithms can realistically handle only mildly nonlinear problems. The Maryland study quantifies exactly how much nonlinearity it can handle with a new parameter, R, which represents the ratio of a problem's nonlinearity to its linearity – its tendency toward chaos versus the friction keeping the system on the rails.

"[Childs' study is] mathematically rigorous. He gives very clear statements of when it will work and when it won't work," Osborne said. "I think that's really, really interesting. That's the core contribution."

The MIT-led study doesn't rigorously prove any theorems to bound its algorithm, according to Kiani. But the team plans to learn more about the algorithm's limitations by running small-scale tests on a quantum computer before moving to more challenging problems.

The most significant caveat for both techniques is that quantum solutions fundamentally differ from classical ones. Quantum states correspond to probabilities rather than to absolute values, so instead of visualizing air flow around every segment of a jet's fuselage, for example, you extract average velocities or detect pockets of stagnant air. "This fact that the output is quantum mechanical means that you still have to do a lot of stuff afterwards to analyze that state," Kiani said.

It's vital to not overpromise what quantum computers can do, Osborne said. But researchers are bound to test many successful quantum algorithms like these on practical problems in the next five to 10 years. "We're going to try all kinds of things," he said. "And if we think about the limitations, that might limit our creativity."

53 Robust quantum computational advantage scheme using fermion sampling

https://www.swissquantumhub.com/robust-quantum-computational-advantage-scheme-using-fermion-sampling/

Fermionic Linear Optics (FLO) is a restricted model of quantum computation which in its original form is known to be efficiently classically simulable.

A team of researchers showed that, when initialized with suitable input states, FLO circuits can be used to demonstrate quantum computational advantage with strong hardness guarantees.

Based on this, they proposed a quantum advantage scheme which is a fermionic analogue of Boson Sampling: Fermion Sampling with magic input states.

They considered in parallel two classes of circuits: particle-number conserving (passive) FLO and active FLO that preserves only fermionic parity and is closely related to Matchgate circuits introduced by Valiant.

Mathematically, these classes of circuits can be understood as fermionic representations of the Lie groups $U(d)$ and $SO(2d)$. They first showed anti-concentration for probabilities in random FLO circuits of both kind. Moreover, they proved robust average-case hardness of computation of probabilities. To achieve this, they have adapted the worst-to-average-case reduction based on Cayley transform, introduced recently by Movassagh, to representations of low-dimensional Lie groups. Taken together, these findings provide hardness guarantees comparable to the paradigm of Random Circuit Sampling.

Most importantly, their scheme has also a potential for experimental realization. Both passive and active FLO circuits are relevant for quantum chemistry and many-body physics and have been already implemented in proof-of-principle experiments with superconducting qubit architectures. Preparation of the desired quantum input states can be obtained by a simple quantum circuit acting independently on disjoint blocks of four qubits and using 3 entangling gates per block.

They have also argued that due to the structured nature of FLO circuits, they can be efficiently certified.

04 Jan 2021

54 Reading out qubits like toppling dominoes: a new scalable approach towards the quantum computer

by C. J. van Diepen

https://qutech.nl/2021/01/04/reading-out-qubits-like-toppling-dominoes-a-new-scalable-approach-towards-the-quantum-computer/

Creating a powerful, large-scale quantum computer depends on a clever design such that many qubits (the building block of a quantum computer) can be controlled and read out. Researchers at QuTech, a collaboration between TU Delft and TNO, have invented a new readout method that is an important step forward on the road towards such a large-scale quantum computer. They have published their findings in Nature Communications today.

Like toppling dominoes

"Our new readout method is based on a phenomenon that all of us know from our childhood: toppling dominoes," said Sjaak van Diepen, PhD researcher in Lieven Vandersypen's group and lead author of the article. "A first transition triggers a second transition, a second transition triggers a third transition, and so on – much like dominoes toppling over in a chain reaction." Considering the implications of this domino-effect led the team to invent a new readout method. It will be able to overcome a major challenge involved in scaling up towards large-scale quantum computers: that of qubit connectivity (the ability to connect many qubits together).

Spin-qubits in quantum dot arrays

The approach of Vandersypen's group to building a quantum computer is based on so-called spin qubits in quantum dot arrays. Quantum dots are very tiny islands that can each confine one or multiple electrons and are tunnel coupled to their neighbours. The spin of the electron acts as a qubit. Spin qubits in quantum dots are read out via a very sensitive detector that measures the charge in its environment. Van Diepen: "Charge sensors work well, but only locally: they need to be in close proximity to the charge they measure. Scaling up the current approach towards a large number of interconnected qubits will therefore limit qubit connectivity, because we would need to place sensors close to all qubits."

Transferring quantum information over a distance

The new readout scheme invented by the scientists makes sure that even a spin qubit far away from the charge sensor will still be read out with high accuracy. Tzu-Kan Hsiao, postdoc and second author of the paper: "Our readout method is based on the fact that charges interact with one another. Therefore, a first charge transition can trigger other charge transitions – forming a cascade of transitions."

Before such a cascade of transitions can occur, the researchers first have to make sure that the electrons become sensitive to those transitions – just as dominoes must be put upright before they can topple over. Van Diepen: "We trigger a first charge transition through a method called spin-to-charge conversion, where one particular spin state will lead to a charge transition. This sets off the cascade of transitions, allowing us to read out the spin of a charge far away from the sensor."

Benefits for research groups and industry

The scientists hope that other research groups and industry working on the development of a quantum computer will benefit from implementing the readout method and build upon their findings. In this way, the challenges on the road towards a large-scale quantum computer can be overcome one by one – just like toppling dominoes.

55 Karnataka to use blockchain for property registration

by Shruthi HM Sastry

https://www.deccanherald.com/state/top-karnataka-stories/karnataka-to-use-blockchain-for-property-registration-934862.html

Property registration in Karnataka is all set to become more secure and hassle-free, with the state government developing a system based on blockchain technology for online property documentation.

The new system, developed in collaboration with IIT-Kanpur, promises an immutable electronic storage of property data through blockchain. In other words, data once stored cannot be changed, eliminating risks of impersonation and unauthorised tweaking of records.

According to Additional Chief Secretary (e-governance) Rajeev Chawla, the new system was approved by the revenue department and would be ready for a pilot in four months. “Unless authorised, no official will be able to tamper with the data,” he said.

Each property holder will be given a property card akin to an ATM card, which can be accessed through a PIN. The property transaction details can be accessed only with the authentication of the user’s digital key or PIN number.

“The content in the blockchain will be locked through this card. The card acts like a locker. Unless the card-based consent is provided, nobody will be able to modify the data,” an expert associated with the project further explained.

From a user’s point of view, this system protects property data besides removing the hassle of storing hard copies of documents. A user will be able to swipe the card at citizen service centres such as Bangalore One and download or print the same.

The new system is expected to strengthen the revenue department’s existing Kaveri portal.

“The identification of a property database in a sub registrar’s office will become easy. Right now, Kaveri depends on human discretion for verification of identity and ownership. A sub-registrar’s office will authenticate all this. The new technology will reduce human discretion as the cards will prove your identity and authentication,” the expert added.

It may be recalled that last year, data pertaining to about 300 properties in the Kaveri portal was allegedly compromised. An internal audit report of the Department of Stamps and Registration suspected that officials with technical expertise had misused the portal.

01 Jan 2021

56 Indian Defense Researchers Report Several Quantum Technology Advances

by Matt Swayne

https://thequantumdaily.com/2021/01/01/indian-defense-researchers-report-several-quantum-technology-advances/

It's been a busy few months in the quantum labs of India's Defense Research & Development Organization (DRDO). The agency has reported significant advances in quantum cryptography and quantum communication, according to their news unit.

Quantum Random Number Generation

The agency reports in a news release that the DRDO Young Scientist Laboratory for Quantum Technologies (DYSL-QT) has developed a Quantum Random Number Generator (QRNG) which detects random quantum events and converts those into a stream of binary digits.

With this development India enters the club of countries who have the technology to achieve the use of quantum technology to generate random numbers. This is important because, according to the agency, random numbers have essential roles in many fields, such as quantum communication, cryptography (key generation, key wrapping, authentication etc.), scientific simulations, lotteries and fundamental physics experiments. The generation of genuine randomness is generally considered impossible with classical means. Quantum mechanics has the inherent potential of providing true random numbers and thus has become the preferred option for the scientific applications requiring randomness.

The laboratory has developed a fiber-optic branch path based QRNG. Branch path-based QRNG relies on the principle that if a single photon is incident on a balanced beam splitter, it will take either of the beam-splitter output paths randomly. As the path chosen by photon is random, the randomness is translated to sequence of bits.

QRNG system developed by the laboratory has been evaluated and verified using several tests, such as DRDO's indigenously developed Randomness Testing Statistical Test Suite of SAG.

Quantum Communication between two DRDO Laboratories

In another advance, DRDO demonstrated secure communication using Quantum Key Distribution (QKD) technology between two DRDO labs in Hyderabad, according to information from the agency.

The team of researchers added that secure communications are vital for defense and strategic agencies world over and distribution of encryption keys from time to time is an important requirement in this context. Sharing of keys over the air or wired links requires encryption, which in turn requires encryption keys to be pre-shared. Quantum based communication offers a robust solution to sharing the keys securely.

The technology is developed by CAIR, Bengaluru and DYSL-QT, Mumbai. Quantum Communication using time-bin Quantum Key Distribution (QKD) scheme was performed under realistic conditions, according to the release. The setup also demonstrated the validation of detection of a third party trying to gain knowledge of the communication. Quantum based security against eavesdropping was validated for the deployed system at over 12kms range and 10dB attenuation over fibre optic channel.

Continuous wave laser source was used to generate photons without depolarization effect. The timing accuracy employed in the setup was of the order of picoseconds. The Single photon avalanche detector

(SPAD) recorded arrival of photons and key rate was achieved in the range of kbps with low Quantum bit error rate. Software was developed for data acquisition, time synchronization, post-processing, determining Quantum bit error rate and extracting other important parameters.

The work being done at DRDO will be used to enable start-ups and SMEs in the domain of Quantum information technologies. It will also serve to define standards and crypto policies that can leverage QKD system in a unified Cipher Policy Committee (CPC) framework for more secure and pragmatic key management for current and future military cryptographic systems.