Crypto News

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

May 1, 2021

Contents

April 2021

30 Apr 2021

1 Ransomware is now a national security risk

by Danny Palmer

https://www.zdnet.com/article/ransomware-is-now-a-national-security-risk-this-group-thinks-it-knows-how-to-defeat-it/

Ransomware is a growing international problem and it needs global cooperation in order to prevent attacks and take the fight to the cyber criminals behind the disruptive malware campaigns.

A paper by the Institute for Security and Technology's (IST) Ransomware Task Force (RTF) – a coalition of cybersecurity companies, government agencies, law enforcement organisations, technology firms, academic institutions and others – has 48 recommendations to help curb the threat of ransomware and the risk it poses to businesses, and society as a whole, across the globe.

Members of the group include Microsoft, Palo Alto Networks, the Global Cyber Alliance, FireEye, Crowdstrike, the US Department of Justice, Europol and the UK's National Crime Agency.

Some of the solutions suggested include governments giving a helping hand to organisations affected by ransomware and providing them with the required cybersecurity support so they don't fall victim in the first place.

Others focus on more direct action, such as taking the fight to ransomware gangs by disrupting their infrastructure, or even regulating Bitcoin and other cryptocurrencies that cyber criminals use to anonymously demand ransom payments from victims.

Ransomware attacks involve cyber criminals compromising the networks of organisations – often via phishing attacks, stolen Remote Desktop Protocol (RDP) credentials or exploiting software vulnerabilities – and then encrypting as many files and servers with malware as possible.

Organisations will in many cases only become aware they've been infected when they see a ransom note on the screens of machines across their network. Often, the victims feel as if they've got no option but to pay the ransom – which can amount to millions of dollars – in order to restore the network.

Ransomware has been around for a number of years, but the cyber criminals behind the attacks are getting bolder, demanding ever-growing ransoms from targets and in many cases blackmailing organisations into payment by threatening to leak sensitive data stolen from the compromised network.

And it isn't just sophisticated criminal gangs that are causing problems; the rise of ransomware as a service means that almost anyone with the skills required to navigate underground forums on the dark web can acquire and use ransomware, safe in the knowledge that they'll probably never face being arrested for their actions.

"The tools are available to malicious actors to ramp up the scale of what they want to do and be able to get away with it. That's what happens as technology diffuses into society and you have inadvertent ramifications which have to be dealt with," says Philip Reiner, executive director of the RTF and CEO of IST.

"We're grappling with that as a global society and we have to come up with better solutions for the problems it presents."

Ransomware isn't new, it's existed in one form of another for decades and the threat has been rising

over the past five years in particular. While it's perceived as a cybersecurity problem, a ransomware attack has much wider ramifications than just taking computer networks offline.

Ransomware attacks are increasingly targeting critical infrastructure, and crucially, over the course of the past year, healthcare.

But many organisations still aren't taking the necessary precautions to protect against ransomware, such as applying security patches, backing up the network or avoiding the use of default login credentials. These concerns are viewed as issues for IT alone, when in reality it's a risk that needs the focus of the entire business.

"We have to stop seeing leaders think of this as a niche computer problem; it's not, it's a whole business event. You should think about ransomware in the same way you think about flooding or a hurricane – this is a thing that will close your business down," says Jen Ellis, vice president of community and public affairs at Rapid7 and one of the RTF working group co-chairs.

"But we don't. We think about it as a niche computer event and we don't recognise the impact it has on the entire business. We don't recognise the impact it has on society."

In 2017, the global WannaCry attack demonstrated the impact ransomware can have on people's everyday lives when National Health Service (NHS) hospitals across the UK fell victim to the attack, forcing the cancellation of appointments and people who came for treatment being turned away.

But years later, the problem of ransomware has got worse and in some cases hospitals around the world are now actively being targeted by cyber criminals.

"You would think there would be no greater wake-up call than that, yet here we are years later having these same conversations. There's a real problem with how people think about and categorise ransomware," says Ellis.

To help organisations recognise the threat posed by ransomware – no matter the sector their organisation is in – the RTF paper recommends that ransomware is designated a national security threat and accompanied by a sustained public-private campaign alerting businesses to the risks of ransomware, as well as helping organisations prepare for being faced with an attack.

But the Ransomware Task Force isn't just suggesting that governments, cybersecurity companies and industry are there to help organisations know what to do if faced by a ransomware attack – one of the key recommendations of the report is for cybersecurity companies and law enforcement to take the fight to the cyber-criminal groups behind the attacks.

A recent operation involving Europol, the FBI and other law enforcement agencies around the world resulted in the takedown of Emotet, a prolific malware botnet used by cyber criminals – and something that had become a key component of many ransomware attacks.

Many cyber criminals switched to using other malware like Trickbot, but some will have taken the fall of Emotet as a sign to give up, because finding new tools makes it that little bit harder to make money from ransomware.

"If you're screwing with infrastructure, like going after Emotet, you're making it harder," says Chris Painter, president of the Global Forum on Cyber Expertise and former senior director for cyber policy at the White House.

In line with this, the paper recommends that the pace of infrastructure takedowns and the disruption of ransomware operations should increase – ultimately with the aim of arrests and bringing criminals who

develop and deploy ransomware to justice.

It's notoriously difficult to apprehend members of ransomware groups, especially when it's an international problem. More often than not, the organisation that comes under a ransomware attack faces an extortion demand from someone who is in another country entirely.

And that's a particular problem for European and North American governments, when large quantities of ransomware attacks by some of the most prolific groups appear to originate from Russia and former-Soviet states – countries that are highly unlikely to extradite suspected cyber criminals.

But identifying cyber criminals isn't impossible – the United States has indicted individuals from Russia for the NotPetya cyberattacks, as well as naming and shaming three North Koreans for their involvement in the WannaCry ransomware attack. Meanwhile, Europol has previously arrested individuals for being involved in ransomware attacks, demonstrating that, while difficult, it isn't impossible to track cyber criminals down and bring them to justice.

One key factor that has allowed ransomware to succeed is that attackers are able to demand payments in Bitcoin and other cryptocurrency. The nature of cryptocurrency means that transactions are difficult to trace and, by the time the Bitcoin has been laundered, it's almost impossible to trace back to the perpetrator of a ransomware attack.

The Ransomware Task Force suggests that in order to make it more difficult for cyber criminals to cash out their illicit earnings, there needs to be disruption of the system that facilities the payment of ransoms – and that means regulating Bitcoin and other cryptocurrency.

"It's recognising that cryptocurrency has a place and there's a reason for it, but also recognising that it's notoriously being used by criminals – is there more that can be done there to make it harder for criminals to use it, or make it less advantageous to them," says Ellis.

Recommendations in the report for decreasing criminal profits include requiring cryptocurrency exchanges to comply with existing laws and to encourage information exchange with law enforcement.

The idea is that by applying additional regulation to cryptocurrency, it allows legitimate investors and users to continue using the likes of Bitcoin and Monero, but makes it harder for cyber criminals and ransomware gangs to use it as an easy means of cashing what they've extorted out of victims – to the extent that, if it's too difficult, they won't bother with attacks in the first place.

"If they're using cryptocurrencies as a way to hide, if you have more compliance with existing regulations, it makes it tougher for them," says Painter.

The paper offers 48 recommendations and has been presented to the White House. It's hoped that with cooperation across the board, businesses can be provided with the tools required to prevent ransomware attacks, governments can get more hands-on with providing help, and law enforcement can hunt down ransomware attackers – but it's only going to work if ransomware is viewed as global problem, rather than one for individual organisations or governments to fight alone.

"What's really important is that this has an international perspective on it, because it's not an American problem, it's an international problem," says Reiner.

2 Goldman Sachs and QC Ware Collaboration Brings New Way to Price Risky Assets Within Reach of Quantum Computers

by Matt Swayne

https://www.thequantumdaily.com/2021/04/30/goldman-sachs-and-qc-ware-collaboration-brings-new-way-to-price-risky-assets-within-reach-of-quantum-computers/

Marking a significant step in the roadmap for quantum advantage for financial applications, Goldman Sachs and QC Ware researchers have designed new, robust quantum algorithms that outperform state-of-the-art classical algorithms for Monte Carlo simulations and can be used on near-term quantum hardware expected to be available in 5 to 10 years.

Monte Carlo methods, used to evaluate risk and simulate prices for a variety of financial instruments, involve complex calculations and consume significant time and computational resources. Typically, these calculations are executed once overnight, which means that in volatile markets, traders are forced to use outdated results. Providing traders, who are always looking for an additional edge in the markets, with a quantum computing approach to perform these risk assessments with far greater speed means that simulations could be executed throughout the day and could transform the way financial markets worldwide operate.

"Our team at Goldman Sachs is focused on developing the best technology for the firm and our clients," said William Zeng, Head of Quantum Research, Goldman Sachs. "Quantum computing could have a significant impact on financial services, and our new work with QC Ware brings that future closer. To do this, we introduced new extensions to a core technique in quantum algorithms. This exemplifies the fundamental contributions that our group looks to make in the field of quantum technology."

The research community has known for some time of quantum algorithms that can perform Monte Carlo simulations 1000× faster than classical methods. However, these algorithms require error-corrected quantum hardware projected to be available in 10 to 20 years. Current quantum devices have very high error rates and can only perform a few calculation steps accurately before returning incorrect results.

For the past year, Goldman Sachs and QC Ware researchers have been working to answer this question: "How can we cut the current timeline in half yet still get a significant speed-up?" By successfully sacrificing some of the speed up from 1000× to 100×, the team was able to produce Shallow Monte Carlo algorithms that can run on near-term quantum computers expected to be available in 5 to 10 years. Technical details of the new algorithms are outlined in a recently released research paper.

Reducing the Quantum Hardware Timeline for Monte Carlo Simulations

The graph below illustrates how Shallow Monte Carlo algorithms compare with previous Monte Carlo algorithms across two dimensions:

- the speed-up provided by the quantum algorithms when compared to classical approaches, and
- the expected timeline for quantum hardware capable of executing the algorithms

The graph also shows the comparative position of two often cited quantum algorithms and their use cases, prime factoring and the variational quantum eigensolver (VQE) algorithms.

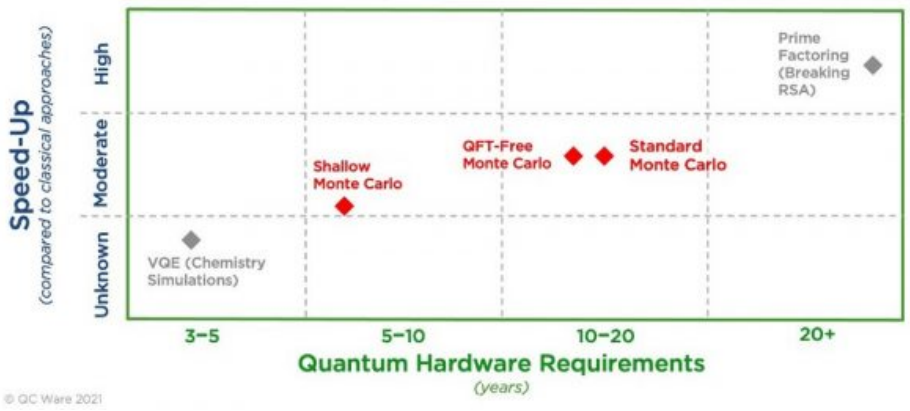

Figure 1: Goldman Sachs and QC Ware teams estimate complex financial modeling may be done on a quantum computer in as early as 5 years.

While the Shallow Monte Carlo algorithms show more moderate speed-ups than Quantum Fourier Transformation Free Monte Carlo (QFT-free Monte Carlo) and Standard Monte Carlo algorithms, they have far less onerous hardware requirements, and therefore are anticipated to reduce the timeline to usability in half.

"At QC Ware, we focus on designing useful quantum algorithms that significantly reduce quantum hardware requirements yet achieve provable performance speed-ups over classical algorithms," said Iordanis Kerenidis, Head of Algorithms – International, QC Ware. "The Goldman Sachs and QC Ware research teams took a novel approach to designing quantum Monte Carlo algorithms by trading off performance speed-up for reduced error rates. Through rigorous analysis and empirical simulations, we demonstrated that our Shallow Monte Carlo algorithms could result in the ability to perform Monte Carlo simulations on quantum hardware that may be available in 5 to 10 years."

29 Apr 2021

3 Governing airspace with quantum-enabled radar

https://www.quantumsensors.org/news/2021/04/29/governing-airspace-with-quantum-enabled-radar

Flying taxis sound improbable but are actually just a short time away from being realised. A recent Economist article highlighted the growing investment being poured into this new vehicle sector across the world, and in the UK, start-up company Vertical Aerospace have announced their collaboration with Rolls Royce to launch their flagship Urban Air Mobility (UAM) electric aircraft.

But disruptive innovation, particularly in an unexplored field, requires discussion around governance and monitoring. Substantial air traffic is a likely possibility in dense areas such as around airports, and designated routes, as well as real-time, resilient and highly accurate monitoring systems, will be required to ensure precise situational awareness.

Researchers at the UK Quantum Technology Hub Sensors and Timing are developing quantum-enabled radar technology, which is currently being tested from the roof of a University of Birmingham campus building to help examine the movement of drones and birds in the airspace. The radar combines incredibly precise quantum science with compact atomic clock oscillators.

These oscillators provide the high precision and low signal noise required for the radar to detect small, slow moving objects at longer distances, and even in cluttered environments. Alongside general monitoring of airspace, quantum radar would be a crucial technology in identifying unmanned aircraft misuse which would potentially put other vehicles in the air and all those beneath at risk.

Hub academics are now developing a novel networked radar system, which would transform surveillance by providing much greater coverage in highly congested environments. The next step for researchers at the Hub is the installation of a second radar on the campus in the autumn, which will represent the next step towards a quantum-enabled radar detection system.

4 Machine learning algorithm helps unravel the physics underlying quantum systems

by University of Bristol

https://phys.org/news/2021-04-machine-algorithm-unravel-physics-underlying.html

Scientists from the University of Bristol's Quantum Engineering Technology Labs (QETLabs) have developed an algorithm that provides valuable insights into the physics underlying quantum systems – paving the way for significant advances in quantum computation and sensing, and potentially turning a new page in scientific investigation.

In physics, systems of particles and their evolution are described by mathematical models, requiring the successful interplay of theoretical arguments and experimental verification. Even more complex is the description of systems of particles interacting with each other at the quantum mechanical level, which is often done using a Hamiltonian model. The process of formulating Hamiltonian models from observations is made even harder by the nature of quantum states, which collapse when attempts are made to inspect them.

In the paper, Learning models of quantum systems from experiments, published in Nature Physics, quantum mechanics from Bristol's QET Labs describe an algorithm which overcomes these challenges by acting as an autonomous agent, using machine learning to reverse engineer Hamiltonian models.

The team developed a new protocol to formulate and validate approximate models for quantum systems of interest. Their algorithm works autonomously, designing and performing experiments on the targeted quantum system, with the resultant data being fed back into the algorithm. It proposes candidate Hamiltonian models to describe the target system, and distinguishes between them using statistical metrics, namely Bayes factors.

Excitingly, the team were able to successfully demonstrate the algorithm's ability on a real-life quantum experiment involving defect centres in a diamond, a well-studied platform for quantum information processing and quantum sensing.

The algorithm could be used to aid automated characterisation of new devices, such as quantum sensors. This development therefore represents a significant breakthrough in the development of quantum technologies.

"Combining the power of today's supercomputers with machine learning, we were able to automatically discover structure in quantum systems. As new quantum computers/simulators become available, the algorithm becomes more exciting: first it can help to verify the performance of the device itself, then

exploit those devices to understand ever-larger systems," said Brian Flynn from the University of Bristol's QETLabs and Quantum Engineering Centre for Doctoral Training.

"This level of automation makes it possible to entertain myriads of hypothetical models before selecting an optimal one, a task that would be otherwise daunting for systems whose complexity is ever increasing," said Andreas Gentile, formerly of Bristol's QETLabs, now at Qu & Co.

"Understanding the underlying physics and the models describing quantum systems, help us to advance our knowledge of technologies suitable for quantum computation and quantum sensing," said Sebastian Knauer, also formerly of Bristol's QETLabs and now based at the University of Vienna's Faculty of Physics.

Anthony Laing, co-Director of QETLabs and Associate Professor in Bristol's School of Physics, and an author on the paper, praised the team: "In the past we have relied on the genius and hard work of scientists to uncover new physics. Here the team have potentially turned a new page in scientific investigation by bestowing machines with the capability to learn from experiments and discover new physics. The consequences could be far reaching indeed."

The next step for the research is to extend the algorithm to explore larger systems, and different classes of quantum models which represent different physical regimes or underlying structures.

28 Apr 2021

5 Bruce Schneier Wants You to Make Software Better

by Daniel Dern

https://spectrum.ieee.org/at-work/tech-careers/bruce-schneier-wants-you-to-make-software-better

Security technologist Bruce Schneier has a warning ""What you code affects the world now. Gone are the days when programmers could ignore the social context of what they code, when we could say, 'The users will just figure it all out.' Today, programs, apps, and algorithms affect society. Facebook's choices influence democracy. How driverless cars will choose to avoid accidents will affect human lives."

Schneier should know, because synthesizing and explaining the impact of technology is what he does. "I work at the intersection of security, technology, and people, mostly thinking about security and privacy policy .... I don't have a single job," says Schneier. "Instead, I do a portfolio of related things."

This includes writing books (14 so far); essays and op-eds; his monthly-since-1998 newsletter and his daily-since-2004 blog; teaching cybersecurity policy at the Harvard Kennedy School; being a fellow at the Berkman Klein Center for Internet and Society at Harvard University; being chief of security architecture at Inrupt; speaking at conferences and events (unsurprisingly, he has done a TED talk); and now and then some security consulting.

"My latest book, **Click Here to Kill Everybody** [2018], is about the security of cyberphysical systems. Everything is turning into a computer – cars, appliances, toys, streetlamps, power plants – and these computers can affect the world in a direct physical manner. Computer security is now about life and property."

Schneier started out in cryptography in the mid-1990s, becoming a public expert after he was laid off from a tech job at AT&T. "I started writing for computer magazines. I wrote cryptography articles for Dr. Dobb's Journal. Then I sold my first book to Wiley – Applied Cryptography [1993] – which became a

bestseller. The book became a 600-page business card, and I started doing cryptography consulting. From there, I generalized to computer security, then network security, then general security technology ... and then to the economics and psychology, sociology, and now, public policy of security."

Schneier does not want to be alone in this work, and encourages others to join him. "We need people who can assess the technologies in social context, how they could impact the real world – and what public policies should address this. To do that, you need to be able to synthesize across technology and policy, and explain this to both technologists and policymakers." And this greater context needs to be factored in at all stages of the software life cycle, "We need social scientists on our software-development teams."

Does this sound appealing? "Where you start out almost doesn't matter. But look outside your silo, look at adjacent or complementary disciplines." As an example, Schneier points to security economics. "I devote a class session on the economics of security. And another on the psychology of security. If you're a security engineer and you don't understand the economic considerations of the problem you're trying to solve, you are going to get the incentives all wrong. And what you create might never get used."

Becoming a good communicator is essential, stresses Schneier. "Explaining technology across interdisciplinary boundaries requires being able to write, speak, to animate a topic, to analogize and synthesize, to summarize and generalize. These are all critical skills. They're not specific skills, but they are vitally important."

27 Apr 2021

6 Silq – The Easier Quantum Computer Programming Language

by Aileen Scott

https://www.thequantumdaily.com/2021/04/27/silq-the-easier-quantum-computer-programming-language/#:~:text=Also%20called%20%E2%80%9Cqfree%E2%80%9D%2C%20Silq,further%20development%20of%20quantum%20computing.&text=The%20algorithms%20in%20Silq%20are,compared%20to%20the%20existing%20languages.

The developers from ETH Zurich, Switzerland have introduced the high-level programming language for quantum computers, called "**Silq**"

This quantum computer programming language tackles the different issues of quantum languages that include unintuitive and cluttered code by supporting safe and automatic uncomputation.

Quantum computing has attained major attention over the last few years, to get the best over the traditional algorithms, many researchers were working on quantum computers and algorithms, which usually function based on the principles of quantum physics which possess huge potential.

Development of Silq

Silq is the first high-level quantum computer programming language, which is specially created around the construction and functionality of the hardware to extract the details from the low-level implementation of quantum algorithms.

With the help of this language, the quantum type system captures the crucial factors of quantum computations and ensures an automatic and safe computation. This is actually a big challenge that current existing quantum languages are facing.

According to computer science professor Martin Vechev and his team of developers at ETH Zurich's Secure, Reliable and Intelligent Systems Lab, "Silq is the first quantum computing language that has a strong-static kind of system that offers intuitive semantics." This can be explained in simple terms as, that if a program type-checks, and then its semantics follows an intuitive recipe that gives temporary values.

This is also a very helpful programming language for quantum computing artificial intelligence as it enables quantum algorithms with more safety and concisely when compared to the existing quantum languages.

Solving the Quantum Programming Problems

One of the best advancements that Silq has brought to the quantum computer programming language is that the issues that the source of errors, which were haunting quantum programming. A computer calculates a problem in many intermediate steps; this gives intermediate results or temporary values. The classical computers erase these values so that they can relieve the memory. The computer scientists called this process "garbage collection," because the superfluous temporary values get disposed of.

Whereas in quantum computers, this type of disposal is tough because of quantum entanglement, the values that were calculated before gets interacted with the present ones, by interfering with the correct calculation. The cleaning of these temporary values on quantum computers calls for an advanced technique for uncomputation.

Silq automatically identifies and erases the values that are no longer required; it is considered the best for optimizing the programming of quantum computers. This process is achieved by the computer scientists through the knowledge of the classical programming languages and applying for their automatic uncomputation process, which only uses programming commands that are free from any type of any special quantum operations. Also called "**qfree**", Silq is very easy to understand, and also very helpful for the further development of quantum computing.

Advantages of Silq

- The algorithms in Silq are shorter and simpler to understand.
- It uses the complete potential of quantum computers compared to the existing languages.
- Silq is safe and automatic uncomputation
- Silq uses code that is quicker, easy, intuitive, and more compact.
- It ensures intuitive yet physical semantics and statically avoids the errors that are not detected in the existing languages.
- It transforms the program's quantum state based on intuitive semantics, which follows the laws of quantum physics.
- Silq also helps with the development of tools for analysis to support developers.
- The programs are less focused on low-level information, this makes analyzing programs in Silq is simpler when compared to the existing languages.
- It easily avoids the notational overhead associated with languages that have lesser static safety in programs.

- Silq enables novel annotations const and qfree
- Silq directly supports the sub-expressions like $(a+b)+c$, whereas the other existing quantum languages make it very tough to directly support.

The prime language features of Silq can also be used in existing languages such as QWire or Q#. Silq is not just easier to write and read but also ensures advancements in numerous tools central to programming quantum computers.

7 How Close is Ordinary Light to Doing Quantum Computing?

by Neil Savage

https://spectrum.ieee.org/tech-talk/computing/hardware/could-ordinary-light-do-quantum-computing.amp.html

Using just a simple laser of the sort found in undergraduate optics labs, physicists may be able to perform some of the same calculations as a hard-to-handle quantum computer operating at ultracold temperatures.

The trick is to use classically entangled light, a phenomenon that has some of the same properties as the traditional entanglement spun out of quantum mechanics. Researchers Yijie Shen from Tsinghua University, Beijing, China, and the University of Southampton, UK, and Andrew Forbes from the University of Witswaterand, Johannesburg, South Africa showed they could create a light beam with multiple entanglements in a recent paper in the journal Light: Science and Applications. And it's all done with mirrors.

"Although it's always spoken about in the quantum world, the idea of entanglement is actually not unique to quantum mechanics," says Forbes, a professor of physics at Witswaterand and leader of the research.

In the quantum realm, entanglement means that two particles – electrons or photons, for instance – have some property that is fundamentally related between the pair. That might be polarization or spin, a quantum property that can be thought of as a bar magnet pointing up or down or somewhere in between. If one particle in an entangled pair is spin up, the other one will be spin down. Measuring one will provide information about the other, even if the particles are on opposite ends of the universe. Those properties are, in the language of physics, non-separable; you can't have one without the other.

In classically entangled light, rather than those non-separable properties being split between two particles, they exist within a single beam of light. "Instead of measuring one property of two photons, you measure two properties of one beam and it comes out to be the same thing," Forbes says.

In this case, the properties are pathways that groups of photons follow within the laser beam. "It's one coherent beam, but following many trajectories in in space," Forbes says. Each of those trajectories is a degree of freedom, and scientists can encode information on those degrees of freedom by assigning each one a different value – instead of the 0s and 1s of digital computing, they might name the different paths 1 through 8 and use those in their calculations.

Classically entangled light, sometimes called "structured light," is not a new concept. But until now no one had entangled more than two properties at once. Forbes says his group's method can entangle a potentially infinite number of pathways, though the limitations of their equipment might impose a practical cap. In their paper, his group demonstrated eight degrees of freedom within one beam.

They do it simply by changing the spacing between mirrors in the laser cavity. One, a fully reflective mirror, is flat, while a second mirror is curved like a lens, and lets some percentage of the photons striking it pass through. When the mirrors are the right distance apart, some of the photons striking it an angle bounce back at the opposite angle, strike the rear mirror, and refract onto the curved mirror at another spot. The photons passing through at different spots on the mirror create the pattern. Simply by moving the mirror, the scientists can change the angles of the light rays and thus the patterns.

"There's an infinite number of paths that you can take – up, down, left, right, diagonal," Forbes says. "Not only could we make light that took many different paths at once, but we could encode information into those paths to make it look like we were holding a high-dimensional multi-photon quantum state."

Because quantum computing relies on particles existing in multiple states, some of the algorithms developed for it could be run using classically entangled light instead, Forbes says. That wouldn't replace the quantum computers researchers are trying to build, but it would provide a bridge between them and the classical computers that now exist. Entangled light could perform more complicated calculations than a digital computer, and do it using bright, easy to handle beams of light, instead of delicate quantum bits that can disappear if they warm up too far beyond absolute zero.

"It will allow us to simulate or possibly even replace some quantum processes in high dimensions which were thought not possible to be done. In other words, just make our life easier," Forbes says. "We're doing quantum like-processes, but with things in the classical world."

26 Apr 2021

8 Towards A Post-Quantum Cryptography

by CNRS

https://scienceblog.com/522461/towards-a-post-quantum-cryptography/

The quantum computing revolution will make many concepts and devices obsolete, thereby generating certain security problems. The National Institute of Standards and Technology in the US has organised an international competition to establish new cryptographic principles. The researcher **Adeline Roux-Langlois** sheds light on the issues involved.

In what ways do quantum technologies pose a threat to cryptography?

Cryptography is based on mathematical problems that are extremely difficult for conventional computers to solve or avoid. However, the quantum machines of the future will be able to do so more easily, making our protection systems obsolete. For now, quantum computers are not powerful or advanced enough to defeat today's cryptographic protocols, but it is important to prepare for them.

The US National Institute of Standards and Technology (NIST), which is in charge of establishing various technological and measurement standards in the United States, launched an international competition in 2017 to build scientific consensus regarding post-quantum cryptography. This process has entered its third and final phase, with both academic and industrial researchers contributing to the effort. Among the sixty-nine initial submissions, the NIST selected those that would make it to the following stage of the competition based on criteria such as security, performance, and the characteristics of the

implementation. It also took into consideration studies published by the scientific community, in addition to possible attacks against each scheme.

What is cryptography currently based on?

There are two approaches for encrypting data, private-key encryption and public-key encryption. In private-key encryption, users share a key. This approach is more secure and less vulnerable to quantum technology, but it is also less practical to use in many cases. The public-key encryption system is based on two keys, one that is kept secret, and another that is available to all. For example, everyone can send encrypted emails to a recipient, who is the only one able to read them. It is nevertheless important to be confident that the problem from which the keys are calculated is sufficiently complex, as any algorithm that can solve it in a reasonable amount of time will provide access to protected data. Ensuring that riddles are difficult enough is the very foundation of security.

Today there are two major types of hard problems, factorisation and discrete logarithm. Factorisation involves decomposing a number into a product of two prime numbers, which is much more tricky than it seems when dealing with very large numbers. Similarly, for the time being no algorithm can effectively calculate a discrete logarithm. The NIST competition is not just limited to encryption. Other algorithms will have to analyse the signature, in other words authenticate the source of a message without being susceptible to falsification. In both cases the criteria clearly include security, but also the system's speed and fluidity.

What approaches have been proposed for post-quantum cryptography?

Various avenues are being pursued. One of them, cryptographic Euclidean networks, involves finding the shortest vectors between two points on a mesh, in a space with hundreds of dimensions. Each vector therefore has a huge number of coordinates, and the problem becomes extremely arduous to solve. Another solution, multivariate cryptography, is based on a somewhat similar principle by proposing to solve polynomials with so many variables that it is no longer possible to calculate within a reasonable time frame. Another approach relies on error-correcting codes, which are used to improve degraded communications, for instance restoring the appearance of a video burned on a DVD that has been damaged. Some of these codes provide a very effective framework for encryption, but function quite poorly when it comes to verifying a signature.

The construction of Euclidean networks is quite present among the finalists, as it works equally well for encryption and signatures. However, everyone in the community does not agree that they should be the focus of attention. The NIST prefers exploring a broad spectrum of approaches for establishing its standards. This way, if a particular solution is attacked, the others will remain secure. For example, the SPHINCS+ algorithm from the Eindhoven University of Technology in the Netherlands, is based on hash functions. A digital fingerprint is ascribed to data, an operation that is extremely difficult to perform in the opposite direction, even using a quantum algorithm. Still, signatures obtained in this way are resource-intensive.

Which French submissions are still in the running for the competition?

There are seven algorithms involving researchers based in France. With regard to encryption, Crystals-Kyber, NTRU, and Saber are based on Euclidean networks, while Classic McEliece rely on error-correcting

codes. Damien Stehlé, a professor at ENS Lyon and a member of the LIP Computer Science Laboratory, and Nicolas Sendrier, from the INRIA research centre in Paris, are taking part in the competition. In the signature category, the Crystals-Dilithium and Falcon algorithms use Euclidean networks, and Rainbow opts for multivariate systems. Stehlé is once again part of the team, as are Pierre-Alain Fouque, a professor at Rennes and member of the IRISA laboratory, as well as Jacques Patarin, a professor at the UVSQ (Université de Versailles-Saint-Quentin-en-Yvelines).

What research are you conducting in these areas?

I focus on cryptography using Euclidean networks, in which I provide theoretical proof that the security of cryptographic constructions is based on problems that are hard enough to be reliable. Encryption and signature are the first applications that come to mind, but it could also be used to ensure the very particular confidentiality of electronic voting, for which the authenticity of votes must be verified before counting, while not revealing who voted for whom. I am also working on anonymous authentication, which for example enables individuals to prove that they belong to a group without disclosing other information, or that they are adults without giving their age or date of birth.

9 Josephson Junction Infrared Single-Photon Detector

by Karine

https://thequantumhubs.com/josephson-junction-infrared-single-photon-detector/

Josephson junctions are simple superconducting devices comprising an insulator or semiconductor separating two superconducting regions. They form the workhorse of superconducting technologies and are exquisitely sensitive to magnetic field.

One long-sought proposal has been to use these devices to detect light.

Although device performance can be degraded by the generation of quasiparticles formed from broken Cooper pairs, this phenomenon also opens opportunities to sensitively detect electromagnetic radiation.

Researchers have realized a photosensitive Josephson junction based on graphene that is capable of sensing single infrared photons.

Such a photosensitive Josephson junction is expected to operate as a high-speed, low-power consumption optical interconnect for communication between superconducting-based supercomputers and quantum computers.

10 Einstein-Podolsky-Rosen (EPR) Paradox And Steering For Quantum-Enhanced Precision Measurements

https://thequantumhubs.com/einstein-podolsky-rosen-epr-paradox-and-steering-for-quantum-enhanced-precision-measurements/

Quantum systems consisting of several particles can be used to measure magnetic or electric fields more precisely. A young physicist at the University of Basel has now proposed a new scheme for such measurements that uses a particular kind of correlation between quantum particles.

In quantum information, the fictitious agents Alice and Bob are often used to illustrate complex communication tasks. In one such process, Alice can use entangled quantum particles such as photons to transmit or "teleport" a quantum state – unknown even to herself – to Bob, something that is not feasible using traditional communications.

However, it has been unclear whether the team Alice-Bob can use similar quantum states for other things besides communication. A young physicist at the University of Basel has now shown how particular types of quantum states can be used to perform measurements with higher precision than quantum physics would ordinarily allow.

Quantum steering describes the fact that in certain quantum states of systems consisting of two particles, a measurement on the first particle allows one to make more precise predictions about possible measurement results on the second particle than quantum mechanics would allow if only the measurement on the second particle had been made. It is just as if the measurement on the first particle had "steered" the state of the second one.

The study of Fadel and his colleagues now makes it possible to systematically study and demonstrate the usefulness of quantum steering for metrological applications. "The idea for this arose from an experiment we already did in 2018 in the laboratory of Professor Philipp Treutlein at the University of Basel," says Fadel.

"In a few simple cases, we already knew that there was a connection between the EPR paradox and precision measurements," Treutlein says. "But now we have a general theoretical framework, based on which we can also develop new strategies for quantum metrology."

Researchers are already working on demonstrating Fadel's ideas experimentally. In the future, this could result in new quantum-enhanced measurement devices.

21 Apr 2021

11 When cryptography attacks – how TLS helps malware hide in plain sight

by Paul Ducklin

https://nakedsecurity.sophos.com/2021/04/21/when-cryptography-attacks-how-tls-helps-malware/

Lots of things that we rely on, and that are generally regarded as bringing value, convenience and benefit to our lives ...

... can be used for harm as well as good.

Even the proverbial double-edged sword, which theoretically gave ancient warriors twice as much fighting power by having twice as much attack surface, turned out to be, well, a double-edged sword.

With no "safe edge" at the rear, a double-edged sword that was mishandled, or driven back by an assailant's counter-attack, became a direct threat to the person wielding it instead of to their opponent.

Sadly, there are lots of metaphorically double-edged swords amidst modern technology.

And no IT technology feels quite as double-edged as encryption, the process of scrambling data securely in such a way that only the intended recipient can ever unscramble it later on.

Almost everything about encryption makes it feel as though it is both immeasurably useful and dispiritingly dangerous at the same time.

The encryption dilemma

Consider some of these dilemmas:

- **You work out how to crack your enemy's "invincible" cipher in wartime.** (The Poles, Swedes, British and others famously and almost unbelievably pulled this off against several Nazi encryption systems during World War 2.) But you daren't let anyone find out how well you're doing, and you can't even use all of the information you decrypt, in case the enemy cottons on and changes the system.
- **You encrypt all the critical data on your computer to protect it from thieves and hackers.** But you'd better not lose the decryption key, or you won't be able to access the information yourself. (Ironically, the stronger and safer the encryption technology you use, the less likely you'll be able to crack it yourself if you ever forget the password.)
- **You implement an encryption system that gives you an advantage over the hackers who keep trying to attack you.** But it's so useful at keeping the hackers out of your business that the hackers start using exactly the same technology themelves, and suddenly you can't keep track of their business, either.

This last dilemma is one that has been creeping up on us steadily over the last few years on the web.

TLS (transport layer security), the protocol used to encrypt the majority of today's web and email traffic, is what puts the padlock in your browser's address bar.

By doing so, TLS makes it very much harder for crooks to do three things:

(i) **The crooks can't easily snoop on the data you're sending** to a website, such as your login password or credit card number.

(ii) **They can't easily tamper with the data that's coming back**, such as altering the bank balance to stop you noticing a fraud, or replacing an innocent download with dangerous malware.

(iii) **They can't easily spoof you** into thinking that their fraudulent, cloned website belongs to a brand or product you trust, such as your bank or a social network.

TLS takes off everywhere

Ten years ago, even the biggest and most popular online services in the world, such as Facebook, Gmail and Hotmail (now Outlook.com) didn't use TLS all the time – it was thought to be too complicated, too slow, and not always necessary.

Sure, social media sites or online stores would encrypt the important stuff, such as when you actually logged in, or paid for something, or edited your private profile.

But the rest of the time, they'd often just use unencrypted web pages, figuring that you didn't really needed protection against snooping, tampering and spoofing when you were "just looking".

Well, that sort of simplification won't wash any more, because we give away more than enough to put us in harm's way just during regular browsing.

These days, therefore, we expect our web browsing to be protected by TLS all the time.

And most of the time these days, it is.

Everything looks the same

Guess what?

The crooks have fallen in love with TLS as well.

By using TLS to conceal their malware machinations inside an encrypted layer, cybercriminals can make it harder for us to figure out what they're up to.

That's because one stream of encrypted data looks much the same as any other.

Given a file that contains properly-encrypted data, you have no way of telling whether the original input was the complete text of the Holy Bible, or the compiled code of the world's most dangerous ransomware.

After they're encrypted, you simply can't tell them apart – indeed, a well-designed encryption algorithm should convert any input plaintext into an output ciphertext that is indistinguishable from the sort of data you get by repeatedly rolling a die.

Paradoxically, then, as more and more of the internet gets encrypted, thus keeping us more secure ...

... it also gets harder and harder to keep track of anomalous, unwanted and dangerous content.

Keeping on top of it all

At this point, you're probably wondering just exactly what the crooks are getting up to these days with TLS, and how much they're using it.

And the excellent news is that Sean Gallagher of SophosLabs has just completed an extensive survey, based on data gathered from all around the world via our own software, to answer exactly those questions.

In his paper, published today, entitled Nearly half of malware now use TLS to conceal communications, he takes you through the tricks used by today's cybercriminals to help them hide in plain sight, simply by making their bad traffic look much the same as our good traffic.

From just under a quarter of malware-related traffic using TLS a year ago to just under half today, this is definitely an issue you should be aware of.

As Sean writes:

> The most concerning trend we've noted is the use of commercial cloud and web services as part of malware deployment, command and control. Malware authors' abuse of legitimate communication platforms gives them the benefit of encrypted communications provided by Google Docs, Discord, Telegram, Pastebin and others – and, in some cases, they also benefit from the "safe" reputation of those platforms.
>
> We also see the use of off-the-shelf offensive security tools and other ready-made tools and application programming interfaces that make using TLS-based communications more accessible continuing to grow.

Learn how these attacks work, and how SophosLabs is able to keep on top of them even though they're encrypted.

12 Genuine Multipartite Entanglement In Noisy Quantum Error Correction Circuits

by Karine

https://thequantumhubs.com/genuine-multipartite-entanglement-in-noisy-quantum-error-correction-circuits/

Ensuring the correct functioning of Quantum Error Correction (QEC) circuits is crucial to achieve fault tolerance in realistic quantum processors subjected to noise.

The first checkpoint for a fully operational QEC circuit is to create Genuine Multipartite Entanglement (GME) across all subsystems of physical qubits.

A team of researchers has introduced a conditional witnessing technique to certify GME that is efficient in the number of subsystems and, importantly, robust against experimental noise and imperfections.

$$g_x^{(1)} = X_1X_2X_3X_4 \qquad g_z^{(1)} = Z_1Z_2Z_3Z_4$$
$$g_x^{(2)} = X_2X_3X_5X_6 \qquad g_z^{(2)} = Z_2Z_3Z_5Z_6$$
$$g_x^{(3)} = X_3X_4X_6X_7 \qquad g_z^{(3)} = Z_3Z_4Z_6Z_7$$

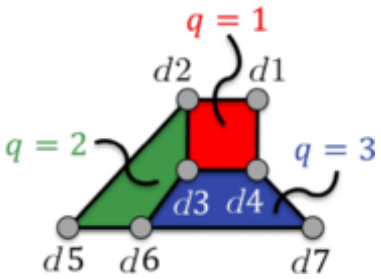

Figure 2: The seven-qubit color code arranged in a three-colorable planar lattice with qubits lying on the vertices, and two types of parity checks per plaquette,

Specifically, they proved that the detection of entanglement in a linear number of bipartitions by a number of measurements that also scales linearly, suffices to certify GME.

Moreover, their method goes beyond the standard procedure of separating the state from the convex hull of biseparable states, yielding an improved finesse and robustness compared to previous techniques. They have applied their method to the noisy readout of stabilizer operators of the distance-three topological color code and its flag-based fault-tolerant version.

In particular, they subjected the circuits to combinations of three types of noise, namely, uniform depolarizing noise, two-qubit gate depolarizing noise, and bit-flip measurement noise. They numerically compared their method with the standard, yet generally inefficient, fidelity test and to a pair of efficient witnesses, verifying the increased robustness of their method.

Last but not least, they have provided the full translation of this analysis to a trapped-ion native gate set that makes it suitable for experimental applications.

20 Apr 2021

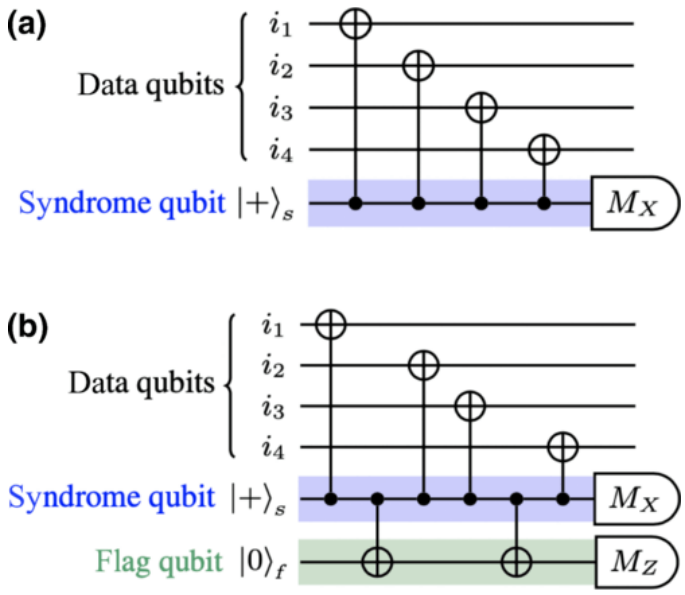

Figure 3: Error syndrome extraction circuits in the color code

13 CaixaBank Develops Risk Classification Model Using Quantum Computing

by Karine

https://thequantumhubs.com/caixabank-develops-risk-classification-model-using-quantum-computing/

CaixaBank is progressing in its preparation strategy for the arrival of quantum computing. After successfully performing the first real tests of quantum computing to study the applications of this technology in financial services, the institution has taken a step further and developed the first machine learning algorithm to classify risks in Spanish banking leveraging Quantum Computing.

The Spanish bank has applied a hybrid computing framework – which combines quantum computing and conventional computing in different phases of the calculation process – to classify credit risk profiles. To do this, CaixaBank used a public data set corresponding to 1000 artificial users, with a similar profile to existing customers, but with information configured specifically for the test.

With this project, the institution is making improvements in risk scenario simulations and machine learning, underpinning increasingly complex algorithms which require large quantities of data to learn, whilst also progressing its analysis of quantum computing applications. The results of this test, which demonstrates that hybrid computing can achieve results comparable to those offered by the conventional solution in less time, will be published in more detail in specialist channels so that the conclusions are available to the community.

Hybrid computing uses this exponential computing advantage to perform complex calculations of parameters optimising machine learning algorithms and combines them with classical computing methods to make the most out of both systems. With the application of hybrid algorithms (quantum and classical) in risk analysis, the institution can reach the same conclusions as the classical method in much less time.

14 Materials Advances Are Key To Development of Quantum Hardware

by Karine

https://thequantumhubs.com/materials-advances-are-key-to-development-of-quantum-hardware/

A new study outlines the need for materials advances in the hardware that goes into making quantum computers. The team of researchers surveyed the state of research on quantum computing hardware with the goal of illustrating the challenges and opportunities facing scientists and engineers.

In practice, the main challenge in realizing quantum computers is that general, many-particle quantum states are highly sensitive to noise, which inevitably causes errors in quantum algorithms. Some noise sources are inherent to the current materials platforms. The team has reviewed some of the materials challenges for five platforms for quantum computers and propose directions for their solution.

This review constitutes a roadmap of the current challenges and opportunities for materials science in Quantum Computing. The scientists have provided a comprehensive review of materials issues in each physical platform by describing the evidence that has led to the current understanding of each problem. For each platform, they have presented reasons for particular material choices, survey the current understanding of sources of noise and dissipation, describe materials limitations to scaling, and discuss potential new material platforms.

Despite major differences among physical implementations in each hardware technology, there are several common themes: Material selection is driven by heterogeneity, impurities, and defects in available materials. Poorly controlled and characterized surfaces lead to noise and dissipation beyond limits imposed by bulk properties. Scaling to larger systems gives rise to new materials problems that are not evident in single-qubit measurements.

They identified three principal materials research frontiers of interest in this context.

- First, understanding the microscopic mechanisms that lead to noise, loss, and decoherence is crucial. This would be accelerated by developing high-throughput methods for correlating qubit measurement with direct materials spectroscopy and characterization.
- Second, relatively few material platforms for solid-state Quantum Information Processing (QIP) have been explored thus far, and the discovery of a new platform is often serendipitous. It is thus important to develop materials discovery pipelines that exploit directed, rational material searches in concert with high-throughput characterization approaches aimed at rapid screening for properties relevant to QIP.
- Third, there are several materials issues that do not affect single-qubit operations but appear as limitations in scaling to larger systems.

Many problems faced by these platforms are reminiscent of some that have been addressed over the past five decades for complementary metal-oxide semiconductor electronics and other areas of the semiconductor industry, and approaches and solutions adopted by that industry may be applicable to QIP platforms. Materials issues will be critical to address in the coming years as we transition from noisy intermediate-scale systems to large-scale, fault-tolerant systems.

15 9 Companies Leading The Quantum Technologies Race in China

by James Dargan

https://thequantumdaily.com/2021/04/20/9-companies-leading-the-quantum-technologies-race-in-china/

Quantum Competitiveness

Nobody needs a Ph.D. in quantum physics to realize the battle of the quantum superpowers is between the US and China.

At present, China is taking the lead when it comes to recruiting the right talent in the sector by its aggressive attitude toward hiring some of America's most talented quantum physicists and other experts. A United States Senate report from 2019, Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans, details in black and white the dangers of China's attitude to this. And though the Chinese have the right as any nation to boost its quantum competitiveness, the White House's complacency here could see it left far behind if it fails to act.

In the commercial scene, too, we can see a changing landscape: according to data in The Quantum Insider (TQI), there are over fifty US quantum computing startups and big players currently active.

China, though far behind this number numerically speaking at the moment, its representation is fair by the standards of most countries.

TQD will now take a look, in alphabetical order, at the main players on the Chinese market. Some of them are pure startups with minimum cash reserves; others tied to the government in some way or subsidiaries of bigger multinationals.

(i) **Baidu Research**

Baidu Research – the research wing of Baidu, Inc., a Chinese multinational technology company specializing in Internet-related services and products and artificial intelligence head-quartered in Beijing's Haidian District – aims to become a world-class Quantum Artificial Intelligence (QAI) research centre by integrating quantum technologies into Baidu's core business through IPs, standards, patents, top acquisition, and research projects in quantum AI, quantum algorithms and quantum architecture.

(ii) **CIQTEK**

Founded in 2016 in the Hefei National High-tech Industry Development Zone, CIQTEK manufactures state-of-the-art quantum sensors, advanced instruments and equipment for analysis and test, technical solutions for enabling industry applications whose customer base includes a global network of private companies, governments and research institutions. CIQTEK's devices will improve outcomes in quantum computation, biology and medicine, food safety, as well as the disciplines of chemistry and material science.

Earlier this year the startup announced that it had raised over 100 million yuan ($15.45 million) in a Series B round of fundraising, The round was led by GL Ventures.

(iii) **Huawei Cloud**

Part Huawei Technologies Co., Ltd. a Chinese multinational technology company with headquarters in Shenzhen, Guangdong Province, Huawei Cloud's New HiQ Quantum Computing Cloud Platform

is enabling Huawei QC research and a future-oriented QC software solution. Providing services for high-performance, large-scale quantum circuit simulation, it is still in beta mode but promises to offer more services in the future.

(iv) **Origin Quantum**

With headquarters in Hefei, Anhui Province, Origin Quantum (officially HeFei Origin Quantum Computing Technology co., LTD) was established in 2017 as a spinoff from the Key Laboratory of Quantum Information at the Chinese Academy of Sciences (CAS) and is led by eminent Chinese quantum computing scientists, Guo Guangcan and Guo Guoping. A full-stack quantum computing company, the startup builds quantum software, quantum chips, quantum measurement devices, quantum control systems, and even a quantum cloud service while also developing its novel IP in quantum AI.

In 2020 the team released its superconducting quantum computer to the world. Called Wu Yuan, it has a 6-qubit superconducting quantum processor. The company also has plans for 24-qubit and 64-qubit devices sometime in the future.

In January of this year, the startup raised more than 100 million Yuan – that's $15 million – in a Series A funding round led by China Internet Investment Fund, a government-affiliated fund, with additional participants in the capital raise of the China Reform Fund and CCB International.

(v) **Qasky**

Qasky, or Anhui Qasky Quantum Technology Co. Ltd, was founded in 2016 by scientists Cai Jiren, Guo Guangcan and Han Zhengfu with the support of the joint investment of Wuhu Construction and Investment Ltd. and the University of Science and Technology of China with the registered capital of 50 million RMB ($7,635m). Based in Wuhu City, Anhui Province, Qasky is commercializing the quantum cryptography research carried out at the Chinese Academy of Sciences and is designing quantum cryptography communication terminal equipment, network switching/routing equipment, core optoelectronic devices/modules, an opening experiment system, scientific instruments, network security control, and application software to provide integrated solutions to quantum information security systems.

Qasky has also built a provincial quantum security project technology research centre, academician workstation, Hefei research and development centre, and other quantum information R&D platforms, and has a proven track record in this area.

(vi) **QuantumCTek**

QuantumCTek Co., Ltd is a leader in commercialized quantum information technology (QIT), designing and manufacturing QIT-enabled ICT security products, services and solutions in telecom infrastructure, enterprise networks, cloud computing, and Big Data technology. QuantumCTek's products have been adopted by government, financial and energy sector players. Based in Hefei, Anhui Province and founded in 2009, it is impressively the first quantum technology company to go public in China

(vii) **QuDoor**

Guokaike Quantum Technology (Beijing) Co., Ltd., more commonly known as Qike Quantum, with the registered trademark QuDoor, designs quantum communication devices and the full-stack development of quantum computers for a customer base that lies in the fields of military, government,

finance, telecommunications, and power. Founded in 2016, QuDoor's cofounder and R&D team have been involved in the development and completion of several quantum information technology feats such as the first commercial quantum communication system (2003), the first dedicated waveform generator for quantum computing (2007), the first to achieve ion trapping on the ion trap chip (2012), the first quantum computing measurement and control system (2015), as well as China's first trapping system with ion-phonon-photon compound entanglement function (2018).

With 32 patents related to quantum information processing technology and a number of non-patent superior technologies, the 50 million yuan ($7.8m) QuDoor raised in an Angel Financing Round earlier this year – made possible by investors Zhongguancun Development Frontier Fund, Zhongguancun Gold Seed Fund and a number of others – will only raise the stakes for the company.

(viii) **Tencent Quantum Lab**

Tencent Quantum Lab, part of the bigger Tencent Holdings Ltd., also known as Tencent, is a Chinese multinational technology conglomerate holding company that was founded in 1998. Based in the technology hub that is the city of Shenzhen, Guangdong Province, Tencent Quantum Lab intends to become the conduit of fundamental theory with practical applications in the fast-growing sector of quantum information technology. Working closely with top universities, research centres, and commercial enterprises globally, Tencent Quantum Lab wants to design and manufacture novel quantum algorithms, systems, software, and cloud services for areas like AI and quantum chemistry.

(ix) **ZTE**

Founded way back in 1985, ZTE Corporation is a partially state-owned global leader in telecommunications and information technology and is listed on both the Hong Kong and Shenzhen Stock Exchanges.

In 2016 ZTE launched the industry's first quantum encryption transport solution based on an optical transport network (OTN).

(x) **Other Players**

With the likes of Kunfeng Quantum Technology and SpinQ based on the Chinese mainland, not to mention the Hong Kong-based M-Labs joining the nine featured, it should be no time at all before we see a flood of startups – both spinoffs from academic institutes and solely private affairs – jumping on board the quantum rollercoaster.

19 Apr 2021

16 Materials advances are key to development of quantum hardware

by Princeton University

https://phys.org/news/2021-04-materials-advances-key-quantum-hardware.html

A new study outlines the need for materials advances in the hardware that goes into making quantum computers if these futuristic devices are to surpass the abilities of the computers we use today.

The study, published in the journal Science by an international team, surveyed the state of research on quantum computing hardware with the goal of illustrating the challenges and opportunities facing scientists and engineers.

While conventional computers encode 'bits' of information as ones and zeroes, quantum computers breeze past this binary arrangement by creating 'qubits,' which can be complex, continuous quantities. Storing and manipulating information in this exotic form – and ultimately reaching 'quantum advantage' where quantum computers do things that conventional computers cannot – requires sophisticated control of the underlying materials.

"There has been an explosion in developing quantum technologies over the last 20 years," said Nathalie de Leon, assistant professor of electrical and computer engineering at Princeton University and the lead author of the paper, "culminating in current efforts to show quantum advantage for a variety of tasks, from computing and simulation to networking and sensing."

Until recently, most of this work has aimed to demonstrate proof-of-principle quantum devices and processors, de Leon said, but now the field is poised to address real-world challenges.

"Just as classical computing hardware became an enormous field in materials science and engineering in the last century, I think the quantum technologies field is now ripe for a new approach, where materials scientists, chemists, device engineers and other scientists and engineers can productively bring their expertise to bear on the problem."

The paper is a call to scientists who study materials to turn to the challenge of developing hardware for quantum computing, said Hanhee Paik, corresponding author and a research staff member at IBM Quantum.

"The progress in quantum computing technologies has been accelerating in recent years both in research and industry," Paik said. "To continue moving forward in the next decade, we will need advances in materials and fabrication technologies for quantum computing hardware – in a similar way to how classical computing progressed in microprocessor scaling. Breakthroughs do not happen overnight, and we hope more people in the materials community will begin to work on quantum computing technology. Our paper was written to give the materials community a comprehensive overview of where we are in materials development in quantum computing with expert opinions from the field."

At the heart of quantum computers are qubits, which work together to churn out results.

These qubits can be made in various ways, with the leading technologies being superconducting qubits, qubits made from trapping ions with light, qubits made from the silicon materials found in today's computers, qubits captured in "color centers" in high-purity diamonds, and topologically protected qubits represented in exotic subatomic particles. The paper analyzed the chief technological challenges associated with each of these materials and proposes strategies for tackling these problems.

Researchers hope that one or more of these platforms will eventually progress to the stage where quantum computing can solve problems that today's machines find impossible, such as modeling the behaviors of molecules and providing secure electronic encryption.

"I think [this paper] is the first time that this kind of comprehensive picture has been assembled. We prioritized 'showing our work,' and explaining the reasoning behind the received wisdom for each hardware platform," de Leon said. "Our hope is that this approach will make it possible for new entrants to the field to find ways to make a big contribution."

The ten co-authors come from research institutions around the world as well as IBM T. J. Watson Research Center, which has a major quantum computing research group. The scientists met during a symposium on materials for quantum computing sponsored by IBM Quantum and the Kavli Foundation and held at the Materials Research Society Fall Meeting in 2019. They then spent much of their time

during the pandemic's stay-at-home period last year developing this review paper.

"It was a great experience to work with a group with such diverse expertise, and a lot of our activity involved asking each other tough questions about why we believed the things we did about our respective material platforms," said de Leon, whose research exploits flaws in diamond materials to enable communication between nodes in a future quantum internet.

18 Apr 2021

17 What's under the hood of a quantum computer?

by Dong Yi, Yang Xiao

https://news.cgtn.com/news/2021-04-18/Tech-It-Out-What-s-under-the-hood-of-a-quantum-computer--Zyl2sLTQIg/index.html

Leading scientists have been seeking a new holy grail – "quantum supremacy." The term "quantum supremacy" does not indicate any technological superiority of one country over another, but rather the enormous computing advantage of quantum computers over classical computers, the latter can vary from the office laptop you type on to those supercomputers that require an entire building to house.

The basic computing increment inside a classical computer is called a "bit," which is based on a binary system that is either 0 or 1. These 0s and 1s constitute the basic bits.

A classical computer can only generate one of these eight values at a time: 000, 010, 001, 011, 110, 100, 101 or 111. Similar to a classical computer, a quantum computer has basic unit of data called a "qubit" or "quantum bit." The qubits can represent numerous possible combinations of 1 and 0 at the same time. This is known as superposition in quantum mechanics.

That's to say, if you ask a normal computer to figure its way out of a maze, it will try every single route in turn. But a quantum computer can go down all the paths at once. That's what makes a quantum computer exponentially mightier than a classical computer.

This is how quantum computing works: A command, which is coded by binary bits, is sent from a classical computer to an electronic converter, where it is turned into microwave signal.

This messenger is shot into a quantum device, where it winds its way down through its entire structure and gradually cooled down to the temperature that's needed. At long last, the messenger reaches the very bottom of the device, where the computing magic actually happens.

The core of a quantum computer is actually just a tiny little chipset, about 1 centimeter in diameter. The chip is where electron, or qubits, are waiting. They received the command and start to communicate with each other to get a computing result. That result is sent out of the device again in the form of microwave signal. It is decoded by a classical computer into a straightforward answer that people prefer.

Quantum computers are not only much more powerful than their classical counterparts, they are also capable of certain tasks impossible for any classical computer to take on, like simulating large atomic and molecular activities in chemical reactions or cracking enigmatic encrypted data.

Critics have been reminding us that this next-gen technology has yet to solve any of our real-life problems. But that may be changing in the next 10 years. With the world-renowned Cleveland Clinic's announcement that it will soon invest in an IBM quantum computer for its future clinical studies, we could be on the verge of a major medical and pharmaceutical breakthrough.

16 Apr 2021

18 Singapore-Based Startup is Focusing on Secure Communication Through QKD & QRNG Technology

by James Dargan

https://thequantumdaily.com/2021/04/16/singapore-based-startup-is-focusing-on-secure-communication-through-qkd-qrng-technology/

Small But Influential

Singapore is one of the most innovative countries in the world when it comes to quantum technologies. And for its geographical size of approximately 730 km^2, this is an impressive achievement. With more than half a dozen startups busy changing the world in the quantum computing (QC) sector, nobody has to make a bet that the trend will only continue well into the future.

CQT Spinoff

One startup which is a good example of both Singaporean innovation and government policy is S-Fifteen Instruments. A spinoff from the Centre for Quantum Technologies (CQT), S-Fifteen Instruments develops photonic quantum technologies for secure communication. Realizing quantum computing (QC) is accelerating at an unprecedented rate and traditional methods of encryption are at serious risk of being breached by them, the S-Fifteen Instruments sees there is no time to waste.

S-Fifteen Instruments

Founded by Lum Chune Yang, Christian Kurtsiefer and Alexander Ling in 2017, the team builds novel solutions to major problems with products in quantum key distribution (QKD), quantum random number generators (QRNGs), entangled photon pair source, and single-photon detectors. To date, the customer base for the quantum control instruments and quantum cryptography hardware is mainly research institutions spread around the globe.

Aligned to the startup's hardware, S-Fifteen Instruments also offers supporting software to "communicate with the host by text commands via a USB-serial interface and open-source scripts in Python available on GitHub.

Lum Chune Yang is the cofounder of S-Fifteen Instruments, as well as being the CEO of another Singapore-based quantum startup, SpeQtral.

A professor at the Physics Department, National University of Singapore (NUS), fellow cofounder Christian Kurtsiefer is simultaneously a principal investigator at CQT.

The last founder of the startup is Alexander Ling, Director of the Quantum Engineering Programme at the National University of Singapore.

With a tight association to the CQT for expert advice at hand, S-Fifteen Instruments is prescient to future threats in cybersecurity issues and is ready to deal with them with products designed to do their job. With the rest of Singapore's innovative atmosphere rubbing off on them, the team's goal is to maintain its current trajectory and while bringing services in QKD and QRNGs to the fore.

19 Federated Quantum Machine Learning

by Karine

https://thequantumhubs.com/federated-quantum-machine-learning/

Distributed training across several quantum computers could significantly improve the training time and if we could share the learned model, not the data, it could potentially improve the data privacy as the training would happen where the data is located.

One of the potential schemes to achieve this property is the Federated Learning (FL), which consists of several clients or local nodes learning on their own data and a central node to aggregate the models collected from those local nodes.

However, to the best of knowledge, no work has been done in Quantum Machine Learning (QML) in FL setting yet.

Researchers have presented the federated training on hybrid quantum-classical machine learning models although their framework could be generalized to pure quantum machine learning model.

Specifically, they have considered the Quantum Neural Network (QNN) coupled with classical pre-trained convolutional model. Their distributed federated learning scheme demonstrated almost the same level of trained model accuracies and yet significantly faster distributed training. It demonstrates a promising future research direction for scaling and privacy aspects.

20 A new piece towards topological quantum computer

by Julien-levallois

https://www.swissquantumhub.com/a-new-piece-towards-topological-quantum-computer/

Each fermion has an antiparticle of opposite electric charge with which it annihilates. But this is not the case for Majorana fermions, which have no charge and are their own antiparticle.

Topological quantum computing is not the most advanced technology, but still quite promising. Indeed, Majorana fermions are ideal candidate for a qubit, because they are very weakly coupled to their environment and they benefit from a very high fidelity rate (quantum operations, measurements) and a very long coherence time. Nevertheless, experimental creation of Majorana fermions is very challenging and their observation can only be done indirectly.

In this theoretical study, published in Physical Review Letters, Rui-Xing Zhang and Prof. S. Das Sarma propose that a quasi-2D thin films of an iron-based superconducting material – FeSCs – would be a high temperature platform for gate-controlled helical topological superconductivity, giving rise to Majorana modes without the need for external proximity effect. In this case, Majorana modes are simply controlled by a magnetic field, which paves the way for the realisation of a topological quantum computer.

21 Dutch researchers establish the first entanglement-based quantum network

https://qt.eu/about-quantum-flagship/newsroom/entanglement-based-quantum-network/

The quantum internet

The power of the Internet is that it allows any two computers on Earth to be connected with each other, enabling applications undreamt of at the time of its creation decades ago. Today, researchers in many labs around the world are working towards the first versions of a quantum internet – a network that can connect any two quantum devices, such as quantum computers or sensors, over large distances. Whereas today's Internet distributes information in bits (that can be either 0 or 1), a future quantum internet will make use of quantum bits that can be 0 and 1 at the same time. 'A quantum internet will open up a range of novel applications, from unhackable communication and cloud computing with complete user privacy to high-precision time-keeping,' says Matteo Pompili, PhD student and a member of the research team. 'And like with the Internet 40 years ago, there are probably many applications we cannot foresee right now.

Towards ubiquitous connectivity

The first steps towards a quantum internet were taken in the past decade by linking two quantum devices that shared a direct physical link. However, being able to pass on quantum information through intermediate nodes (analogous to routers in the classical internet) is essential for creating a scalable quantum network. In addition, many promising quantum internet applications rely on entangled quantum bits, to be distributed between multiple nodes. Entanglement is a phenomenon observed at the quantum scale, fundamentally connecting particles at small and even at large distances. It provides quantum computers with their enormous computational power and it is the fundamental resource for sharing quantum information over the future quantum internet. By realizing their quantum network in the lab, a team of researchers at QuTech – a collaboration between Delft University of Technology and TNO – is the first to have connected two quantum processors through an intermediate node and to have established shared entanglement between multiple stand-alone quantum processors.

Operating the quantum network

The rudimentary quantum network consists of three quantum nodes, at some distance within the same building. To make these nodes operate as a true network, the researchers had to invent a novel architecture that enables scaling beyond a single link. The middle node (called Bob) has a physical connection to both outer nodes (called Alice and Charlie), allowing entanglement links with each of these nodes to be established. Bob is equipped with an additional quantum bit that can be used as memory, allowing a previously generated quantum link to be stored while a new link is being established. After establishing the quantum links Alice-Bob and Bob-Charlie, a set of quantum operations at Bob converts these links into a quantum link Alice-Charlie. Alternatively, by performing a different set of quantum operations at Bob, entanglement between all three nodes is established.

Ready for subsequent use

An important feature of the network is that it announces the successful completion of these (intrinsically probabilistic) protocols with a "flag" signal. Such heralding is crucial for scalability, as in a future quantum

internet many of such protocols will need to be concatenated. 'Once established, we were able to preserve the resulting entangled states, protecting them from noise,' says Sophie Hermans, another member of the team. 'It means that, in principle, we can use these states for quantum key distribution, a quantum computation or any other subsequent quantum protocol.'

15 Apr 2021

22 SKT to Launch 5G Smartphone with Integrated Quantum Cryptography

by ray sharma

https://www.thefastmode.com/services-and-innovations/19529-skt-to-launch-5g-smartphone-with-integrated-quantum-cryptography

SK Telecom this week announced that it will introduce the Galaxy Quantum2, its second smartphone equipped with quantum cryptography technology, in cooperation with Samsung.

The company will open pre-order for the Galaxy Quantum2 from April 13 to 19, 2021 and officially launch the device on April 23, 2021 in Korea.

With features matching to those of Samsung's flagship smartphones - i.e. a 6.7-inch display, 64MP camera, Qualcomm Snapdragon 855 plus chipset, along with strengthened quantum cryptography technologies, the Galaxy Quantum2 will be a new choice for customers who value both performance and security, said SK Telecom.

Like its predecessor the Galaxy A Quantum, the Galaxy Quantum2 is equipped with the world's smallest quantum random number generator (QRNG) chipset measuring 2.5mm by 2.5mm developed by ID Quantique, SKT's strategic partner in quantum cryptography communication technology. This QRNG chipset allows smartphone holders to use services that require security in a more safe and secure manner by generating unpredictable and patternless true random numbers.

The Galaxy Quantum2 is expected to provide differentiated security experience to customers by dramatically expanding the number of services that can be applied with quantum cryptography. That is, services that are based on Android Keystore (APIs) will be automatically secured by QRNG.

For instance, SKT's services like T World, PASS and T Membership, as well as mobile banking services of Shinhan Bank and Standard Chartered Bank Korea will be securely provided through the use of quantum cryptography. Going forward, SKT plans to further expand QRNG-applicable services to include those provided by financial companies like Samsung Card and SKT's music streaming service FLO and video ringback tone service V Coloring.

14 Apr 2021

23 A Novel Light-Spin Interface Advances Development Of Quantum Computers

by Karine

https://thequantumhubs.com/a-novel-light-spin-interface-advances-development-of-quantum-computers/

Researchers at Karlsruhe Institute of Technology (KIT) and Chimie ParisTech/CNRS have now significantly advanced the development of molecule-based materials suitable for use as light-addressable fundamental quantum units.

They have demonstrated for the first time the possibility of addressing nuclear spin levels of a molecular complex of europium(III) rare-earth ions with light.

The molecule, which belongs to the rare earth metals, is designed to exhibit luminescence, i.e., a europium(III)-centered sensitized emission, when excited by ultraviolet light-absorbing ligands surrounding the center.

After light absorption, the ligands transfer the light energy to the europium(III) center, thereby exciting it. Relaxation of the excited center to the ground state leads to light emission.

The whole process is referred to as sensitized luminescence. Spectral hole burning – special experiments with lasers – detect the polarization of the nuclear spin levels, indicating the generation of a efficient light-nuclear spin interface. The latter enables the generation of light-addressable hyperfine qubits based on nuclear spin levels.

13 Apr 2021

24 AWS reveals a new method to build a more accurate quantum computer

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/aws-reveals-a-new-method-to-build-a-more-accurate-quantum-computer/

Amazon's cloud subsidiary AWS has released its first research paper detailing a new architecture for a future quantum computer, which, if realized, could set a new standard for error correction.

The cloud company published a new blueprint for a fault-tolerant quantum computer that, although still purely theoretical, describes a new way of controlling quantum bits (or qubits) to ensure that they carry out calculations as accurately as possible.

The paper is likely to grab the attention of many experts who are working to improve quantum error correction (QEC), a field that's growing in parallel with quantum computing that seeks to resolve one of the key barriers standing in the way of realising useful, large-scale quantum computers.

Quantum systems, which are expected to generate breakthroughs in industries ranging from finance to drug discovery thanks to exponentially greater compute capabilities, are effectively still riddled with imperfections, or errors, that can spoil the results of calculations.

The building blocks of quantum computers, qubits, exist in a special, quantum state: instead of representing either a one or a zero, like the bits found in classical devices, quantum bits can exist in both states at the same time. While this enables a quantum computer to carry out many calculations at once, qubits are also highly unstable, and at risk of collapsing from their quantum state as soon as they are exposed to the outside environment. Consequently, the calculations performed by qubits in quantum

gates cannot always be relied upon – and scientists are now exploring ways to discover when a qubit has made an error, and to correct the mistake.

"The quantum algorithms that are known to be useful – those that are likely to have an overwhelming advantage over classical algorithms – may require millions or billions of quantum gates. Unfortunately, quantum gates, the building blocks of quantum algorithms, are prone to errors," said AWS Center for Quantum Computing research scientists Patricio Arrangoiz-Arriola and Earl Campbell in a blog post.

"These error rates have decreased over time, but are still many orders of magnitude larger than what is needed to run high-fidelity algorithms. To reduce error rates further, researchers need to supplement approaches that lower gate error rates at the physical level with other methods such as QEC."

There are different ways to carry out quantum error correction. The conventional approach, known as active QEC, uses many imperfect qubits (called 'physical qubits') to correct one qubit that has been identified as faulty, to restore the particle to a state of precision. The controllable qubit created in this way is called a 'logical qubit'.

Active QEC, however, creates a large hardware overhead in that many physical qubits are required to encode every logical qubit, which makes it even harder to build a universal quantum computer comprising large-scale qubit circuits.

Another approach, passive QEC, focuses on engineering a physical computing system that has an inherent stability against errors. Although much of the work around passive QEC is still experimental, the method aims to create intrinsic fault-tolerance that could accelerate the construction of a quantum computer with a large number of qubits.

In the new blueprint, AWS's researchers combine both active and passive QEC to create a quantum computer that, in principle, could achieve higher levels of precision. The architecture presents a system based on 'cat states' – a form of passive QEC where qubits are kept in a state of superposition within an oscillator, while pairs of photons are injected and extracted to ensure that the quantum state remains stable.

This design, according to the scientists, has been shown to reduce bit-flip error, which occurs when a qubit's state flips from one to zero or vice versa. But to further protect qubits from other types of error that might arise, the researchers propose coupling passive QEC with known active QEC techniques.

Repetition code, for example, is a well-established approach to detect and correct error in quantum devices, which Arrangoiz-Arriola and Campbell used together with cat states to improve fault tolerance in their theoretical quantum computer.

Promising results, challenges ahead

The results seem promising: the combination of cat states and repetition code produced an architecture in which just over 2,000 superconducting components used for stabilization could produce a hundred logical qubits capable of executing a thousand gates.

"This may fit in a single dilution refrigerator using current or near-term technology and would go far beyond what we can simulate on a classical computer," said Arrangoiz-Arriola and Campbell.

Before the theoretical architecture proposed by the researchers takes shape as a physical device, however, several challenges remain. For example, cat states have already been demonstrated in the lab in previous proof-of-concept experiments, but they are yet to be produced at a useful scale.

The paper nevertheless suggests that AWS is gearing up for quantum computing, as major tech players increasingly enter what appears to be a race for quantum.

IBM recently unveiled a roadmap that eyes a 1121-qubit system for 2023, and is currently working on a 127-qubit processor. Google's 54-qubit Sycamore chip made headlines in 2019 for achieving quantum supremacy; and Microsoft recently made its cloud-based quantum ecosystem, Azure Quantum, available for public preview.

Amazon, for its part, launched an AWS-managed service called Amazon Braket, which allows scientists, researchers and developers to experiment with computers from quantum hardware providers, such as D-Wave, IonQ and Rigetti. However, the company is yet to build its own quantum computer.

12 Apr 2021

25 NVIDIA Announces SDK for Quantum Simulation on GPUs

https://quantumcomputingreport.com/nvidia-announces-sdk-for-quantum-simulation-on-gpus/

One very useful tools for those wishing to develop quantum programs is a classical computing based simulator that can demonstrate how a quantum computer would process the program. Although the drawback of this approach is that it is limited to the number of qubits the classical computer can simulate, but it has the advantage is that the classical computing simulations can be performed on an in-house system and not require submitting a job to some quantum computer in the cloud. The simulations can also be done in an error-free environment so that programs can be initially developed to check out the basic logic without a programmer having to deal with noisy qubits that can cause uncertainty when analyzing the results of a run. Although a real quantum computer with full error correction could accomplish the same thing, this would require machines that have thousands of qubits and won't be available for many years.

In order to improve the performance of these simulations, a recent trend is to utilize GPUs (Graphics Processing Units) and other special processors to execute these simulations more efficiently than general purpose processing units. Because quantum operations can be described using matrix mathematics and tensor networks, the architecture of GPUs is better optimized to process these types of operations.

To this end, NVIDIA has just announced an SDK (Software Development Kit) called **cuQuantum** that provides simulation capabilities on NVIDIA's latest GPUs. The package contains APIs that allow one to create a quantum program in one of the common frameworks such as Qiskit, Cirq, ProjectQ, Q#, and others and then simulate it on a platform that contains one of the recent generation of NVIDIA GPUs. The SDK currently supports two different methods of simulation. The State Vector Simulator provides high fidelity results, but requires a memory space that grows 2^n with the number of qubits and limits the total number of qubits that can be simulated The Tensor Network method trades memory footprint for memory to allow one to simulate a program with a larger number of qubit at a slightly reduced fidelity. NVIDIA will continue development of this SDK and will be releasing additional simulation capabilities in the future.

The performance of this approach can be quite good. As an example NVIDIA worked with Caltech to simulate Google's 53 qubit Sycamore processor with a circuit that had a depth of 20, similar to the one used in Google's quantum supremacy experiment and were able to complete the simulation in 9.3 minutes

on NVIDIA in-house Selene supercomputer. Google's experiment took a little over 3 minutes on Sycamore and estimated that replicating it on Oak Ridge's Summit supercomputer would take 10,000. However, to be fair, the full Google experiment required running it for 1,000,000 shots while the NVIDIA/Caltech 9.3 minute run was just for one shot. This is still a substantial improvement over the Summit estimate and it is likely that fewer shots would be needed to get a valid answer in the GPU simulation because it doesn't have noisy qubits.

26 Critical security alert: If you haven't patched this old VPN vulnerability, assume your network is compromised

by Danny Palmer

https://www.zdnet.com/article/critical-security-alert-if-you-havent-patched-this-two-year-old-vpn-vulnerability-assume-your-network-is-compromised/

Cyber criminals and nation-state cyber-espionage operations are actively scanning for unpatched vulnerabilities in Fortinet VPNs; organisations that use Fortigate firewalls on their network, and have yet to apply a critical security update released almost two years ago, should assume they've been compromised and act accordingly.

The alert from the National Cyber Security Centre (NCSC) follows a report by Kaspersky detailing how cyber criminals are exploiting a Fortinet VPN vulnerability (CVE-2018-13379) to distribute ransomware by exploiting unpatched systems and remotely accessing usernames and passwords, allowing them to manually undertake activity on the network.

The NCSC – along with CISA and the FBI – has also warned that Advanced Persistent Threat (APT) nation-state hacking groups are still actively scanning for unpatched CVE-2018-13379 vulnerabilities as a means of gaining access to networks for cyber-espionage campaigns.

Fortinet issued a critical security update to counter the security vulnerability after it was discovered in 2019, but almost two years later a significant number of organisations have yet to apply the patch to their enterprise network, leaving them vulnerable to cyberattacks.

Cyber criminals have published a list of almost 50,000 IP addresses relating to unpatched devices; the NCSC warns that 600 of these are in the UK and that the organisations running them are "at very high risk of exploitation".

In fact, the NCSC has warned that organisations using unpatched Fortinet VPN devices must assume they are now compromised, and should begin incident management procedures. That includes removing the device from service and returning it to factory settings, as well as investigating the network for suspicious or unexpected activity.

"This recent activity emphasises the importance of NCSC advice to install security updates as soon as is practicable following their release to ensure action is taken before exploitation is observed," said the alert.

The NCSC recommends that all Fortinet VPN users check whether the 2019 updates have been installed, and if they haven't to apply them immediately to prevent cyber attackers from exploiting the vulnerability.

"The security of our customers is our first priority. For example, CVE-2018-13379 is an old vulnerability resolved in May 2019. Fortinet immediately issued a PSIRT advisory and communicated directly with customers and via corporate blog posts on multiple occasions in August 2019, July 2020, and again in

April 2021 strongly recommending an upgrade," a Fortinet spokesperson told ZDNet.

"If customers have not done so, we urge them to immediately implement the upgrade and mitigations," Fortinet added.

27 Fraunhofer launches quantum computing research platform in Germany

by Janis Eitner

https://www.fraunhofer.de/en/press/research-news/2021/april-2021/fraunhofer-launches-quantum-computing-research-platform-in-germany.html

Considered a game changer, quantum computing will generate knowledge and create new opportunities in many sectors of industry within just a few years: for optimization and simulation, in logistics and transport, energy management, chemistry, medicine or materials science. There is broad consensus in Germany about the huge potential of this future technology. The political, industrial and scientific worlds are working to advance quantum computing to be able to solve practical problems more efficiently sometime soon. Until now, there has been no secure research platform on which companies and institutions can try out quantum-based research strategies, optimize their fields of application and develop the skills they need by training on the system. The quantum computer in Ehningen in Baden-Württemberg is now offering such a platform.

Setting a milestone for technological sovereignty

"If we want to actively help shape the fast-paced advancements in quantum computing, we in Germany must now develop the expertise required for the various application scenarios, as well as the compatible algorithms and the all important new business models," explains Prof. Reimund Neugebauer, President of the Fraunhofer-Gesellschaft. "With our platform around the IBM quantum computer and our Competence Network Quantum Computing, we are offering all companies and research institutions the opportunity to play an active part in advancing this future technology, gather the expertise they need to thrive in the quantum age and apply the newly acquired skills to good advantage."

"Here at IBM, we are convinced that open technologies and an active and global community of developers, scientists and experts from industry, government and universities are the key to the success of the quantum computer," says Gregor Pillen, General Manager IBM Germany, Austria and Switzerland. "The first installation of an IBM Quantum System One in Europe will accelerate progress in this field and give companies of all sizes access to the technology as they prepare to enter the quantum computer era."

German Federal Minister of Education and Research Anja Karliczek explains: "Quantum technologies will bring about lasting and fundamental changes in science, business and society. Quantum sensors, quantum communication or even quantum computing – all of these emerging technologies will enable solutions for those scientific, economic and social problems that have long seemed unsolvable. For example, quantum communication will make completely secure data transmission a reality. The German Federal Ministry of Education and Research promotes quantum technologies through its own initiatives and funding announcements, such as the QuNET project for completely secure communication, in order to facilitate the transfer of quantum technologies into everyday applications for business and society and to secure Germany's and Europe's technological sovereignty. I am doing all that I can to make sure that we decisively

and quickly advance the critical field of quantum technologies and develop ready-to-use mature technology in Germany. The Federal Research Ministry can rely on the Fraunhofer-Gesellschaft and its institutes as an important partner in the German research landscape for this undertaking."

Minister-President of Baden-Württemberg Winfried Kretschmann says: "The quantum computer is an important step for the state of Baden-Württemberg on its journey to successfully shaping key future technologies and meeting the challenges of the digital age. With this initiative, we are contributing to a German quantum technology ecosystem with international magnetic appeal, and setting a milestone for the technological sovereignty of Germany and of Europe. We want to use the opportunities quantum computing offers for applications in industry and science at the earliest possible stage. Quantum computers hold huge potential for the fields of research and experimentation: This technology can optimize traffic flows and logistical processes, analyze complex financial flows more efficiently, simulate new chemical models or accelerate innovations in the medical and energy sectors."

State Minister of Economic Affairs, Dr. Nicole Hoffmeister-Kraut, emphasizes: "Baden-Württemberg has the benefit of an established network of excellent quantum science at universities and applied research institutions, as well as an internationally leading high-tech industry. With our knowledge, we are making a significant contribution to the progress and use of quantum computing. Quantum algorithms are opening up brand new opportunities and much more efficient approaches – in the engineering, material and data sciences for example. To develop these fields for profitable applications in our country, we are collaborating with Fraunhofer and IBM to create access to what is currently Europe's most powerful quantum computer in Ehningen."

10 Apr 2021

28 Quantum Photonics Breakthrough Promises a New Era of Powerful Optical Circuits

by university of southern california

https://scitechdaily.com/quantum-photonics-breakthrough-promises-a-new-era-of-powerful-optical-circuits/

The modern world is powered by electrical circuitry on a "chip" – the semiconductor chip underpinning computers, cell phones, the internet, and other applications. In the year 2025, humans are expected to be creating 175 zettabytes (175trillion gigabytes) of new data. How can we ensure the security of sensitive data at such a high volume? And how can we address grand-challenge-like problems, from privacy and security to climate change, leveraging this data, especially given the limited capability of current computers?

A promising alternative is emerging quantum communication and computation technologies. For this to happen, however, it will require the widespread development of powerful new quantum optical circuits; circuits that are capable of securely processing the massive amounts of information we generate every day. Researchers in USC's Mork Family Department of Chemical Engineering and Materials Science have made a breakthrough to help enable this technology.

While a traditional electrical circuit is a pathway along which electrons from an electric charge flow, a quantum optical circuit uses light sources that generate individual light particles, or photons, on-demand, one-at-a-time, acting as information carrying bits (quantum bits or qubits). These light sources are nano-sized semiconductor "quantum dots"–tiny manufactured collections of tens of thousands to a million atoms

packed within a volume of linear size less than a thousandth of the thickness of typical human hair buried in a matrix of another suitable semiconductor.

They have so far been proven to be the most versatile on-demand single photon generators. The optical circuit requires these single photon sources to be arranged on a semiconductor chip in a regular pattern. Photons with nearly identical wavelength from the sources must then be released in a guided direction. This allows them to be manipulated to form interactions with other photons and particles to transmit and process information.

Until now, there has been a significant barrier to the development of such circuits. For example, in current manufacturing techniques quantum dots have different sizes and shapes and assemble on the chip in random locations. The fact that the dots have different sizes and shapes mean that the photons they release do not have uniform wavelengths. This and the lack of positional order make them unsuitable for use in the development of optical circuits.

In recently published work, researchers at USC have shown that single photons can indeed be emitted in a uniform way from quantum dots arranged in a precise pattern. It should be noted that the method of aligning quantum dots was first developed at USC by the lead PI, Professor Anupam Madhukar, and his team nearly thirty years ago, well before the current explosive research activity in quantum information and interest in on-chip single-photon sources. In this latest work, the USC team has used such methods to create single-quantum dots, with their remarkable single-photon emission characteristics. It is expected that the ability to precisely align uniformly-emitting quantum dots will enable the production of optical circuits, potentially leading to novel advancements in quantum computing and communications technologies.

The work, published in APL Photonics, was led by Jiefei Zhang, currently a research assistant professor in the Mork Family Department of Chemical Engineering and Materials Science, with corresponding author Anupam Madhukar, Kenneth T. Norris Professor in Engineering and Professor of Chemical Engineering, Electrical Engineering, Materials Science, and Physics.

“The breakthrough paves the way to the next steps required to move from lab demonstration of single photon physics to chip-scale fabrication of quantum photonic circuits,” Zhang said. “This has potential applications in quantum (secure) communication, imaging, sensing and quantum simulations and computation.”

Madhukar said that it is essential that quantum dots be ordered in a precise way so that photons released from any two or more dots can be manipulated to connect with each other on the chip. This will form the basis of building unit for quantum optical circuits.

“If the source where the photons come from is randomly located, this can’t be made to happen.” Madhukar said.

“The current technology that is allowing us to communicate online, for instance using a technological platform such as Zoom, is based on the silicon integrated electronic chip. If the transistors on that chip are not placed in exact designed locations, there would be no integrated electrical circuit,” Madhukar said. “It is the same requirement for photon sources such as quantum dots to create quantum optical circuits.”

“This advance is an important example of how solving fundamental materials science challenges, like how to create quantum dots with precise position and composition, can have big downstream implications for technologies like quantum computing,” said Evan Runnerstrom, program manager, Army Research Office, an element of the U.S. Army Combat Capabilities Development Command’s Army Research Laboratory. “This shows how ARO’s targeted investments in basic research support the Army’s enduring modernization efforts in areas like networking.”

To create the precise layout of quantum dots for the circuits, the team used a method called SESRE (substrate-encoded size-reducing epitaxy) developed in the Madhukar group in the early 1990s. In the current work, the team fabricated regular arrays of nanometer-sized mesas (Fig. 1(a)) with a defined edge orientation, shape (sidewalls) and depth on a flat semiconductor substrate, composed of gallium arsenide (GaAs). Quantum dots are then created on top of the mesas by adding appropriate atoms using the following technique.

First, incoming gallium (Ga) atoms gather on the top of the nanoscale mesas (black arrows in (b)) attracted by surface energy forces, where they deposit GaAs (black outline on mesa top, (b)). Then, the incoming flux is switched to indium (In) atoms, to in turn deposit indium arsenide (InAs) (red region in (b)), followed back by Ga atoms to form GaAs and hence create the desired individual quantum dots (upper image in (b)) that end up releasing single photons. To be useful for creating optical circuits, the space between the pyramid-shaped nano-mesas needs to be filled by material that flattens the surface. The final chip is shown schematically in (c), where opaque GaAs is depicted as a translucent overlayer under which the quantum dots are located.

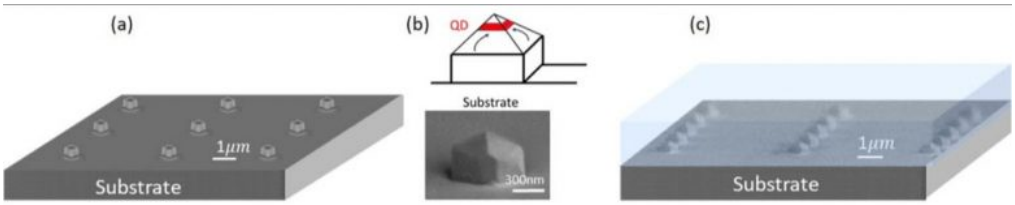

Figure 4: (a) Scanning electron microscope (SEM) image of starting nanometer-sized mesa array created on a flat semiconductor substrate; (b) Schematic of mesa profile evolution during material deposition with the black arrows indicating atom migration direction leading first to GaAs size-reduction (the SESRE approach) and then switching to the deposition of quantum dot material InAs (red) on the size-reduced mesa top and back to GaAs to bury the red InAs; A SEM image of the mesa bearing the single quantum dot is shown below; (c) Indicates the realized quantum dot array buried under a planarized GaAs surface shown symbolically as a translucent overlayer to enable visualization (GaAs is opaque).

"This work also sets a new world-record of ordered and scalable quantum dots in terms of the simultaneous purity of single-photon emission greater than 99.5%, and in terms of the uniformity of the wavelength of the emitted photons, which can be as narrow as 1.8nm, which is a factor of 20 to 40 better than typical quantum dots," Zhang said.

Zhang said that with this uniformity, it becomes feasible to apply established methods such as local heating or electric fields to fine-tune the photon wavelengths of the quantum dots to exactly match each other, which is necessary for creating the required interconnections between different quantum dots for circuits.

This means that for the first time researchers can create scalable quantum photonic chips using well-established semiconductor processing techniques. In addition, the team's efforts are now focused on establishing how identical the emitted photons are from the same and/or from different quantum dots. The degree of indistinguishability is central to quantum effects of interference and entanglement, that underpin quantum information processing – communication, sensing, imaging, or computing.

Zhang concluded: "We now have an approach and a material platform to provide scalable and ordered sources generating potentially indistinguishable single-photons for quantum information applications. The approach is general and can be used for other suitable material combinations to create quantum dots emitting over a wide range of wavelengths preferred for different applications, for example fiber-based optical communication or the mid-infrared regime, suited for environmental monitoring and medical

diagnostics," Zhang said.

Gernot S. Pomrenke, AFOSR Program Officer, Optoelectronics and Photonics said that reliable arrays of on-demand single photon sources on-chip were a major step forward.

"This impressive growth and material science work stretches over three decades of dedicated effort before research activities in quantum information were in the mainstream," Pomrenke said. "Initial AFOSR funding and resources from other DoD agencies have been critical in realizing the challenging work and vision by Madhukar, his students, and collaborators. There is a great likelihood that the work will revolutionize the capabilities of data centers, medical diagnostics, defense and related technologies."

29 Finnish Quantum Institute Announced: InstituteQ to Coordinate Research, Education and Innovation Across Country

by Matt Swayne

https://thequantumdaily.com/2021/04/10/finnish-quantum-institute-announced-instituteq-to-coordinate-research-education-and-innovation-across-country/

Aalto University, University of Helsinki and VTT Technical Research Centre of Finland have signed an agreement to collaborate on quantum science and technology, under the umbrella of InstituteQ: The Finnish Quantum Institute. InstituteQ brings together expertise in research, education, and innovation to drive Finland's world-leading quantum technology research.

'Our goals are threefold,' explains Professor Jukka Pekola, Aalto University,

- 'firstly, to coordinate our national research efforts;
- secondly, to provide the best possible education, both in graduate and industrial programs; and
- thirdly, in driving innovation.'

'It is widely recognised that the expertise level in the workforce is currently a major bottleneck in developing quantum technology,' explains Professor Sabrina Maniscalco, University of Helsinki, 'By combining and coordinating our resources, we will be able to grow expertise in new directions.'

All three of the founder institutions have decades of experience in the research, teaching and commercialisation of quantum science and technology. By joining forces through InstituteQ, the parties aim to keep Finland and Europe at the forefront of an increasingly competitive global field.

'We see exponential and sustainable growth opportunities in quantum technologies for the future. We want to be inclusive and invite interested stakeholders – companies and institutions alike – across Finland to join. InstituteQ will be a global window of Finnish quantum expertise and facilitate new, international collaborations' said Himadri Majumdar, VTT, 'Our aim is to all work together to leverage Finland's quantum expertise to create new opportunities – for both research, and business.'

Supporting a growing ecosystem

'Quantum technology' is the application of phenomena that arise from the unique behaviour of quantum physics. The most widely recognised technology is quantum computing: making computers that can solve

problems that are impossible for regular computers to solve. Quantum computing will be useful for problems like designing new medicines, securing digital communication and data storage, and others. Developing quantum computing requires whole new types of hardware, software and communication technologies, with completely different logic from conventional computers.

Aalto University, University of Helsinki and VTT are already strong global leaders in the research and development of the technology needed for quantum systems, such as devices and sensors, novel quantum materials, and quantum information. Finland is currently building a 3-stage Quantum Computer in a co-development project led by VTT and together with Finnish start-up IQM. The project showcases Finnish expertise and provides an initial platform for both further research, innovation and commercial activities.

'Finnish companies are already working in this area, both as technology enablers providing the hardware and software to exploit quantum phenomena; and as end-users providing services that use quantum technology to customers' explains Dr Majumdar, 'at InstituteQ we want to work with both.'

'We have a lot of students, both domestic and international who are interested in studying quantum technology' continues Professor Maniscalco. 'By supporting the creation of new professorships and national educational programs across our partner institutions we will be able to grow the expertise here in Finland that industry and academia need to harness the capabilities of quantum technology.'

'In Finland, we already have a strong environment for quantum technology, such as the OtaNano research infrastructure and the QTF Centre of Excellence' says Professor Pekola, 'We want the Institute to guide the development of current infrastructure, and have a role in generating new pathways and projects for quantum technologies. We are looking forward to growing the institute to include more partners, collaborators and stakeholders from across research and industry in Finland. Together we can get the maximum benefit out of our great research environment, and develop it further to meet the needs of the future.'

09 Apr 2021

30 US blacklists seven Chinese supercomputer groups

https://www.bbc.com/news/business-56685136

It is the first move by the Biden administration to make it harder for China to obtain US technology

On Thursday, three companies and four branches of China's National Supercomputing Center were added to the US blacklist.

This bars American companies from exporting technology to the groups without proper approval.

The US commerce department said the groups were involved in building supercomputers used by Chinese "military actors" and facilitating programmes to develop weapons of mass destruction.

The sanctioned groups are leading China's supercomputing development and are key players in Beijing's plan for chip self-sufficiency.

US Commerce Secretary Gina Raimondo said the Biden administration would use "the full extent of its authorities to prevent China from leveraging US technologies to support these destabilising military modernisation efforts".

The Trump administration had also targeted dozens of Chinese companies it suspected of using American technology for military uses, including phonemaker Huawei.

Mr Biden's move on Thursday requires the seven Chinese groups to obtain licences to access American technologies, including chip infrastructures designed by Intel and other U.S chipmakers.

While the blacklist bars US-based companies from providing services and products to the Chinese firms, it doesn't bar those that are produced in facilities outside of the US.

One such company is **TSMC**, the Taiwan-based company that has become the world's most advanced semiconductor manufacturer.

What is a supercomputer?

Supercomputers have a considerably higher level of performance compared to a general-purpose computer and can make billions of calculations per second.

Supercomputers are made up of thousands of connected processors and are used for functions like forecasting weather and climate trends, simulating nuclear tests and for pharmaceutical research.

They are also necessary for the development of advanced weapons such as hypersonic missiles.

"Supercomputing capabilities are vital for the development of many – perhaps almost all – modern weapons and national security systems, such as nuclear weapons and hypersonic weapons," Ms Raimondo added.

'Not waiting around'

The US is worried about China gaining access to American technology that helps its army close the gap with the US military.

The Biden administration is currently reviewing dozens of China-related actions that Donald Trump took, including an order that prohibits Americans from investing in Chinese companies believed to be linked to the military.

"Do you think China is waiting around to invest in its digital infrastructure or research and development? I promise you, they are not waiting," Mr Biden said in a speech on Wednesday.

Mr Biden said China and the rest of the world "are racing ahead of us in the investments they have in the future".

31 IBM's new tool lets developers add quantum-computing power to machine learning

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/ibms-new-tool-lets-developers-add-quantum-computing-power-to-machine-learning/

IBM is releasing a new module as part of its open-source quantum software development kit, Qiskit, to let developers leverage the capabilities of quantum computers to improve the quality of their machine-learning models.

Qiskit Machine Learning is now available and includes the computational building blocks that are necessary to bring machine-learning models into the quantum space.

Machine learning is a branch of artificial intelligence that is now widely used in almost every industry. The technology is capable of crunching through ever-larger datasets to identify patterns and relationships, and eventually discover the best way to calculate an answer to a given problem.

Researchers and developers, therefore, want to make sure that the software comes up with the most optimal model possible – which means expanding the amount and improving the quality of the training data that is fed to the machine-learning software. This process inevitably comes with higher costs and much longer training times.

Delegating some parts of the process to a quantum computer could resolve these issues, by speeding up the time it takes to train or evaluate a machine-learning model, but also by vastly increasing what is known as the feature space – the collection of features that are used to characterize the data that is fed to the model, for example "gender" or "age" if the system is being trained to recognize patterns about people.

While classical computers are limited by the compute power required by large features spaces, quantum computers are expected to – once the technology is mature enough – excel at taking on large calculations in a short amount of time.

With quantum computing still in its early days, much of the work around quantum machine learning is theoretical, and still dependent on the scaling up of quantum devices in the future; but a growing number of researchers are nevertheless showing interest in delving deeper into the opportunities that the technology could one day unlock.

"Quantum computation offers another potential avenue to increase the power of machine-learning models, and the corresponding literature is growing at an incredible pace," said the Qiskit applications team. "Quantum machine learning proposes new types of models that leverage quantum computers' unique capabilities to, for example, work in exponentially higher-dimensional feature spaces to improve the accuracy of models.

"Using classical and quantum machine-learning models may allow researchers to better understand quantum chemistry and physics, opening up plenty of new applications and research directions."

Even for the most savvy machine-learning developer, however, jumping into the world of quantum can be a daunting prospect – which is why Qiskit released the new module, with the promise that the program's design enables developers to prototype a model even without expert knowledge of quantum computing.

For example, Qiskit Machine Learning provides QuantumKernel, a tool that computes kernel matrices for a given dataset into a quantum framework. This is the first step towards mapping data into an exponentially higher-dimensional feature space that can provide more accurate training for machine-learning models.

The new module also contains multiple implementations of quantum neural networks, as well as learning algorithms to train and use them, so that developers can construct and test their own networks.

Finally, Qiskit Machine Learning allows users to integrate their new quantum neural networks directly into the PyTorch open-source machine-learning library. A Facebook-developed platform, the PyTorch library is primarily used for applications such as computer vision and natural language processing.

In effect, as Qiskit's applications team explained, quantum machine learning is expected to work in tandem with classical computing, with compute-heavy tasks run on quantum devices to improve models designed for classical applications.

"They can be part of a bigger complex computation, such as a deep neural network that consists of classical as well as quantum layers," said the team. "This opens endless opportunities to investigate the potential power of quantum neural networks for a vast number of applications."

Once they have built a quantum machine-learning model in Qiskit, developers will be able to test the algorithm on classical computers, but also on IBM's cloud-based quantum systems. The first release of Qiskit Machine Learning provides a starting selection of models, but, since the platform is an open-source library, the applications team encouraged researchers and developers to get to work to start growing the body of research.

08 Apr 2021

32 Zurich Instruments introduces a new generation of signal generators for quantum computing

by Julien Levallois

https://www.swissquantumhub.com/zurich-instruments-introduces-a-new-generation-of-signal-generators-for-quantum-computing/

The SHFSG Signal Generator is an instrument designed to control superconducting and spin qubits and reach higher fidelities with less overhead time. As the first solution of its kind on the market, the SHFSG operates directly at qubit frequencies without mixer calibration. The SHFSG sets new standards in spectral purity and stability, and ensures that the highest possible gate fidelity is achieved and maintained during operation. As an integral component of the Zurich Instruments Quantum Computing Control System, the SHFSG provides a scalable solution for controlling quantum processors.

Concept

- **Hardware**

  The SHFSG generates freely programmable pulse sequences on up to 8 outputs with a signal bandwidth of 1 GHz and a variable carrier frequency up to 8.5 GHz. Such microwave signals are required to control the state of qubits in quantum computers, and they previously had to be generated using a combination of arbitrary waveform generators, microwave signal generators, and mixer circuits. The SHFSG brings together all these instruments in a single box, and it eliminates the need for time-consuming and error-prone calibration routines.

  "The SHFSG sits in the sweet spot between meeting the specialized needs of today's researchers and keeping an eye on the roadmap for scaling up in the future. It addresses the improvements that truly matter for research teams in quantum computing, yet it is also an instrument versatile enough to cover the variety of approaches pursued in different quantum technology endeavors," says Dr. Mark Kasperczyk, Application Scientist for Quantum Technologies at Zurich Instruments. Through its ZSync interface and low-latency dynamic sequencing capabilities, the SHFSG supports feedback methods such as active reset and quantum error correction. The ZSync protocol also enables precise and reproducible timing synchronization across instruments, ensuring that gate operations on separate channels are well-aligned even for systems of up to 144 qubit control channels. The instrument comes in a 4- and an 8-channel variant to suit all setup sizes.

The SHFSG represents an important step toward standardized operation of today's largest quantum processors. It requires a minimum amount of memory to generate complex signals, hence it reduces the instrument's communication time – an otherwise critically limiting factor in the tune-up procedures of large quantum computing systems.

"The SHFSG is the result of long-standing and intensive collaborations with some of Europe's leading quantum computing groups," says Dr. Paolo Navaretti, Product Manager at Zurich Instruments. "These collaborations established the application know-how that has allowed us to identify the right choices at all levels of product design."

- **Software support and integration**

  As part of the Quantum Computing Control System (QCCS), the SHFSG is seamlessly integrated into setups featuring the HDAWG Arbitrary Waveform Generator and the SHFQA Quantum Analyzer. The LabOne QCCS Software allows users to define multi-channel signals involving all instruments in the setup in the form of a pulse-level description abstracted from the hardware. The LabOne user interface, already known to Zurich Instruments' customers, gives access to an overview of all hardware settings and to the instrument-level sequence description.

33 Honeywell makes the demonstration of the trapped-ion quantum CCD computer architecture

by Julien Levallois

https://www.swissquantumhub.com/honeywell-makes-the-demonstration-of-the-trapped-ion-quantum-ccd-computer-architecture/

Trapped-ions is considered as one of the most promising mean to create most usable quibits, because it requires only a single ion crystal in a single trapping region. Unfortunately, it appears that this approach is unlikely to scale beyond 100 qubits. Developing an architecture allowing scalable trapped-ion quantum computer is therefore quite challenging.

By integrating all necessary elements of the trapped-ion quantum charge-coupled device (QCCD) architecture into a programmable trapped-ion quantum computer, authors realised simple quantum operation as a teleported CNOT gate and obtain negligible crosstalk error and a quantum volume of $2^6 = 64$.

Even if the realisation of large systems of thousands or millions of qubits remains challenging and uncertain, this demonstration provides a viable path towards high-performance quantum computers.

07 Apr 2021

34 Future of Quantum computing

by Sanjam Singh

https://medium.com/quantum-london/future-of-quantum-computing-1f23d693bde1

Quantum computers really do represent the future generation of computing. Cloud-based quantum computing is tougher to drag off than AI, therefore the ramp-up is going to be slower, and therefore

the learning curve vessel attributable to the rather nebulous science behind it, a sensible, operating quantum computer remains a flight of fancy. Bits are the elemental computing units, however, they will store only two values 0 and 1. Developers use quantum computing to encrypt issues as qubits, that work out multiple mixtures of variables promptly instead of exploring every possibility discretely. The deployment of quantum circuits and therefore the support systems necessary for their operation could be an expensive and troublesome process. Among the scope of the analysis, firms that already use these systems modify cloud-based quantum computing via the platforms they build.

Many startups and technology giants, together with Microsoft, IBM, and Google, acknowledge the worth of creating progress during this field, as this is often so successive major step in technology and computing. Quantum computers area unit lightning-fast compared to a typical Windows 10 computer or a macOS computer that makes them even quicker than the foremost powerful supercomputers we have these days. Once users area unit allowed to access quantum physics-powered computers via the web, then it's quantum computing within the cloud. Rigetti computing could be a startup that has developed a quantum processor that's in operation and Computing 128 qubits. They recently declared a Quantum Cloud Service, that developed on its existing quantum computing within the Cloud programming toolkit. This service can bring each ancient and quantum computer along on one cloud platform to assist users to build applications exploitation the ability of qubit technology. Applications of quantum computing will be –

- **Machine Learning / Big data:** ML and profound learning analysts are looking for productive approaches to prepare and test models utilizing huge informational collection. Quantum registering can assist with making the way toward preparing and testing quicker.
- **Simulation:** Reenactment is a helpful instrument to expect potential blunders and make a move. Quantum processing techniques can be utilized to mimic complex frameworks.
- **Optimization:** Numerous streamlining issues are looking for a worldwide negligible point arrangement. By utilizing quantum strengthening, the advancement issues might be addressed sooner than utilizing supercomputers.
- **Material Science:** Science and material science are restricted by the computations of the mind-boggling connections of nuclear designs. Quantum arrangements are promising a quicker method to show these collaborations.

Main subjects for quantum computing

- **Quantum Cloud:** Cloud-based quantum registering is a strategy for giving quantum figuring by utilizing emulators, test systems, or processors through the cloud. Quantum registering frameworks cover enormous volumes and work temperatures at only 15 millidegrees above outright zero. Given the trouble of sending these frameworks, it is a need with the present innovation to do the activities wanted to be performed absurd.
- **Quantum Neural Networks(QNN):** QNNs is a mix of old-style counterfeit neural organization models with the benefits of quantum processing to create productive calculations. QNN is for the most part hypothetical recommendations without full actual execution. utilizations of QNN calculations can be utilized in demonstrating networks, memory gadgets, and computerized control frameworks.
- **Quantum Cryptography:** Quantum cryptography means building up a protected encryption strategy by exploiting quantum mechanical properties. Quantum cryptography expects to make it

difficult to decipher a message utilizing traditional strategies. For instance, if anybody attempts to duplicate quantum encoded information, the quantum state is changed while attempting to endeavor.

- **Quantum Circuits:** A quantum circuit comprises quantum doors, instatement, and reset structures that empower quantum tasks and counts on quantum information. A qubit can be considered as a unit of data and the quantum circuit is the unit of calculation. As quantum circuits are created to make quantum computations boundless, the force of quantum figuring will be reflected in everyday life.
- **Quantum Optics:** Quantum optics is a territory that inspects the communication of photons with particles and molecules. Further exploration regarding this matter answers issues experienced in semiconductor innovation and correspondence. Thusly, quantum figuring can empower further improvement of old-style PCs.
- **Quantum Cognition:** Quantum Cognition expects to demonstrate ideas like the human mind, language, dynamic, human memory, and applied thinking by utilizing quantum figuring. Quantum discernment depends on different psychological wonders characterized by the quantum hypothesis of data to depict the cycle of dynamic utilizing quantum probabilities.

Why it is important for the future?

- **More mind-boggling issues are emerging:** As innovation progresses, the issues experienced are getting more perplexing. Quantum processing offers an answer for complex issues like protein displaying. The most recent worldwide emergency brought about by Coronavirus shows that researchers need an alternate device to display a solitary protein and deactivate it. Another illustration of a dramatic ascent in complex issues can be energy utilization. As the human populace increments and the utilization rate increments dramatically, more mind-boggling issues like streamlining of sources are emerging. Quantum PCs can be utilized to experience the limits of complex issues by utilizing the material science of quantum mechanics.
- **Supercomputers are restricted to taking care of nonlinear issues:** Traditional processing is a helpful device for performing successive tasks and putting away data. Notwithstanding, it is hard to track down answers for turbulent issues since it is displayed dependent on straight math. Quantum processing is by all accounts an appropriate possibility for taking care of nonlinear issues as it has nonlinear properties of nature. That being said, quantum PCs are not appropriate for a wide range of calculations.

35 Quantum computers will win the next world war

by Tristan Greene

https://thenextweb.com/neural/2021/04/07/quantum-computers-will-win-next-world-war-3-three-artificial-intelligence-ai/

What would happen if an AI gained control of the US military's nuclear stash and decided to preemptively win World War 3 before any perceived enemy nations could react?

Fans of cinema from the 1980s may recognize that query as the plot to the classic science-fiction film[1] "Wargames" starring a young Matthew Broderick. It was a great but terribly silly movie that paired nicely with popcorn and suspended disbelief. Nevertheless, the question it asked remains valid.

In the film, the AI is eventually stymied by Boolean logic after attempting to "win" against itself at Tic-Tac-Toe. Those who understand how AI actually works might find the entire plot of the movie preposterous, but the ending is especially chuckle-worthy. At least it used to be.

Today's computers use binary logic so, in essence, everything's a yes or no question to an AI running classic algorithms. Even when researchers design AI that "rates" things, they usually just break the degrees between ratings down into yes-or-no questions for the AI to answer in increments.

But tomorrow's AI won't be stuck in the mire of classical physics. Useful quantum computers are just around the corner – they should be here sometime between next Tuesday and the year 2121.

With quantum computers, our military systems won't be constrained to yes-or-no questions and they certainly won't have to run boring old binary simulations to determine the confidence factor for a given operation.

Prasanth Shyamsundar, a researcher at the Fermi National Accelerator Laboratory, a Department of Energy research lab for the US government, recently published a fascinating paper describing two new types of algorithms that could revolutionize quantum computing and, potentially, lead to a quantum brain for military AI systems.

A press release from Fermi describes what the algorithms do by invoking the image of an AI sorting through a stack of 100 assorted vinyl records to find the sole jazz album. Under the normal AI paradigm, a deep learning system would be trained on what jazz sounds like and then it would parse each record individually until one of them meets a pass/fail threshold for jazz.

The first of the algorithms Shyamsundar proposes would, essentially, allow that same AI to sort through the entire stack of albums at the same time.

Quantum AI isn't smarter, it's just fast and takes advantage of "superposition." Where classical AI works in a black box, quantum AI could exploit superposition to operate in many black boxes at once.

Unfortunately, that doesn't mean it comes up with the right answer. When it's a yes-or-no question, the odds are good. But when it's a question that requires non-Boolean logic, such as rating 100 albums for their jazzyness on a scale of 1-10, even a quantum computer needs a different kind of algorithm.

And that's what the second algorithm does, according to Shyamsundar.

Per a press release from the Fermi lab:

> A second algorithm introduced in the paper, dubbed the quantum mean estimation algorithm, allows scientists to estimate the average rating of all the records. In other words, it can assess how "jazzy" the stack is as a whole.
>
> Both algorithms do away with having to reduce scenarios into computations with only two types of output, and instead allow for a range of outputs to more accurately characterize information with a quantum speedup over classical computing methods.

To be clear, Shyamsundar's work has nothing to do with military operations and the Fermi lab, as mentioned, belongs to the DoE (not the DoD). Their paper represents the groundwork towards basic

[1]Note: Spoilers ahead because the movie is more than 30 years old

functioning quantum algorithms.

But what is a military AI technology if not an innocuous, basic algorithm persisting?

The problem with today's military logic systems – and the one in the movie "Wargames" – is that they're all based on binary thinking.

You can run a million simulations on advanced military software using cutting-edge AI, but eventually the limitations of "pass/fail" thinking will reduce almost any conflict into an arms race that ends in either stalemate or mutually-assured destruction.

But, what if the confidence factor for a given military operation didn't rely on binary simulations? The same quantum algorithms that can determine which album in a given stack is a jazz album 10 times faster than a binary system, and how jazzy a given album is, could easily determine which combination of feasible operational strategies would result in the highest overall confidence factor for a military campaign.

In other words, where Sun Tzu was said to be able to envision an entire battle unfolding in front of his eyes before it happened, and modern software such as CMANO can simulate entire operations, a quantum system running simple non-Boolean algorithm solutions should be able to surface strong predictions for the outcome of a multi-step war campaign.

36 Honeywell releases details of its ion trap quantum computer

by john timmer

https://arstechnica.com/science/2021/04/honeywell-releases-details-of-its-ion-trap-quantum-computer/

About a year ago, Honeywell announced that it had entered the quantum computing race with a technology that was different from anything else on the market. The company claimed that because the performance of its qubits was so superior to those of its competitors, its computer could do better on a key quantum computing benchmark than quantum computers with far more qubits.

Now, roughly a year later, the company finally released a paper describing the feat in detail. But in the meantime, the competitive landscape has shifted considerably.

It's a trap!

In contrast to companies like IBM and Google, Honeywell has decided against using superconducting circuitry and in favor of using a technology called "trapped ions." In general, these use a single ion as a qubit and manipulate its state using lasers. There are different ways to create ion trap computers, however, and Honeywell's version is distinct from another on the market, made by a competitor called IonQ (which we'll come back to).

IonQ uses lasers to perform its operations, and by carefully preparing the light, its computer can perform operations on multiple qubits at the same time. This essentially allows any two qubits in its system to perform a single operation and lets IonQ build up a complicated entangled system. It's a contrast to the behavior of quantum computers that use superconducting circuits, where each qubit is typically only connected directly to its nearest neighbors.

Honeywell's approach also allows any two qubits to be connected with each other. But it does so by physically moving ions next to each other, allowing a single pulse of light to strike both of them simultaneously.

This works because Honeywell's ion traps aren't made from a static arrangement of magnetic fields. Instead, the fields are generated using 192 electrodes that can all be controlled independently. This allows the device to create locations where the magnetic field varies in strength, leading to the creation of a location where the ion is happier to reside – technically termed a "potential well." By changing the charge in these electrodes, the potential wells can be made to move up and down the linear device, and the ions will simply move with them.

By merging two potential wells, the ions they contain can be brought together, allowing one operation to simultaneously affect them both. When that is done, the well can be split, taking the ions back to their original location.

What's new in the paper are some hard performance numbers on how well this all works. Honeywell says that the maximal amount of time needed to transport an ion from one end of the trap to the other is 300 microseconds. Errors in transport – sending a qubit to the wrong location, for example – are detected automatically by the system, allowing the whole thing to be reset and calculations to be picked up from the last point where the machine's state was read. These errors are also extremely rare. In a series of 10,000,000 operations, a transport failure was detected only three times.

Competition at volume

But that isn't the last of the performance figures documented here. Honeywell also turned to quantum volume, a measure originally defined by IBM that takes into account the number of qubits, how connected they are, and how well they avoid generating errors instead of the intended outcome. If the system can perform operations involving random pairs of its qubits without error two-thirds of the time, its quantum volume is two raised to the power of the qubit count. Higher error rates lower the quantum volume; more qubits raise it.

In this case, the Honeywell team ran tests with two, three, four, and six of the device's qubits. All of them successfully cleared the hurdle, with error-free operation typically in the area of 75 percent for the different qubit counts. Given the six qubits, that results in a quantum volume of 64, which, at the time the manuscript was submitted for review, was a record high.

But again, at that time. There's some good news from Honeywell's perspective, in that the company has added more qubits without increasing the error rate, bringing itself up to a quantum volume of 512. By comparison, IBM only reached Honeywell's earlier mark of 64 this past summer using a machine with 27 qubits but a higher rate of errors.

But there's also the other ion trap computing company, IonQ. Previously, it had been in a similar place to IBM: more qubits, but more errors. However, it managed to roughly triple the qubit count at the same time that it raised its qubit quality to be comparable to Honeywell's. With low errors and the large boost in qubit count, its quantum volume comes in at over 4 million, which is quite a bit higher than 512. And while it took about a year for Honeywell to add two qubits, at the time of its announcement, IonQ said it expects to double its qubit number to 64 within eight months – which is now less than three months away.

Room for improvement

That said, Honeywell has clearly identified where the bottlenecks reside. One problem is the noise in the voltage generators that feed power into the electrodes that control the ions. Another is spontaneous noise in the system. Clean up either of those and the performance goes up.

In addition, moving the ions around imparts some energy to them, requiring them to be constantly cooled down again while the machine is in operation. To prevent the cooling process from disturbing the qubits, Honeywell traps a second ion from a different element at the same time and cools that, turning it into an energy sponge for its partner. This is a major time sink while the machine is in operation, so boosting its efficiency would speed up operations.

Beyond that, the basic control system scales up linearly – literally, but only up to a point. Add more electrodes in line with the rest and you can simply trap more atoms. The point where this scaling ends is when it takes too long to move an atom from one end of the row to the other if needed. It's not clear when that point will be reached, but Honeywell is already considering ideas like two-dimensional arrays of traps and transferring ions between devices.

In any case, the publication itself is informative in two ways. It takes what was an excited corporate announcement a year ago and finally provides the details needed to fully appreciate what was done, and with the validation of peer review. But, the fact that the system that was used to generate the results has become badly obsolete in the time it took the paper to get through peer review gives us a real sense of how exciting the field has become.

06 Apr 2021

37 Toppan and ISARA Partner to Develop Post-Quantum Public Key Cryptography on Smart Cards

https://www.toppan.com/en/news/2021/04/newsrelease210406e.html

Toppan Printing (Toppan), a global leader in communication, security, packaging, décor materials, and electronics solutions, and ISARA Corporation (ISARA), are launching a partnership for the joint development of smart cards equipped with post-quantum public key cryptography.

The public key cryptosystems widely used today will be vulnerable to attacks from large-scale quantum computers, which are expected to come into practical use around 2030. Toppan and ISARA aim to equip smart cards with public key cryptosystems that are secure against attacks from quantum computers to ensure secure verification of access authentication. In collaboration with Japan's National Institute of Information and Communications Technology (NICT), further assessment is planned of the feasibility of smart cards equipped with post-quantum public key cryptography on H-LINCOS, a testbed of quantum secure cloud technology. These activities aim to promote the use of quantum secure cloud technology and to provide services and solutions for secure backup and communication of highly sensitive digital information.

Background

As the digital society accelerates, smart cards, which are used for various access authentication applications, are growing in importance. Smart cards are equipped with public key cryptosystems such as RSA for authentication, but with the anticipated practical application of quantum computing technology within the next 10 years, there is a risk that existing public key cryptography could be decrypted. This has given rise to a need for public key cryptosystems that are secure against quantum computing attacks.

Details of the collaboration

Toppan and ISARA are leveraging expertise in smart card security and authentication technology in a pioneering attempt to equip smart cards with post-quantum public key cryptography. Access authentication using such smart cards is a groundbreaking technology with the potential to revolutionize economies and societies around the world. Early development and rollout will contribute to creating and maintaining infrastructure for safe and secure information communication. Success in establishing the technology will have a significant impact on every environment in which smart cards are used, helping to ensure secure access authentication and enhancing security for society in the future.

Specifically, the project aims to develop a program for smart cards to implement post-quantum algorithms that generate and verify digital signatures and to verify the functionality and applicability to smart cards. Toppan and ISARA will also investigate the feasibility of adapting this smart card technology for use in quantum secure cloud technology. The two companies intend to begin the integration of post-quantum public key cryptography into smart cards and perform the technical verification of authentication systems in 2022, targeting limited practical application in 2025 and the launch of services in 2030.

Roles of each organization

- **Toppan**

  Through the development and manufacture of smart cards, Toppan has accumulated a range of smart card security technologies, including encryption, authentication, and unauthorized access prevention. Leveraging this expertise, Toppan will work to contribute to the establishment of a safe and secure society in the age of quantum computing through support for the application of post-quantum public key cryptography to smart cards and the expanded use of quantum secure cloud technology, as well as the provision of services and solutions such as secure backup and data distribution for highly sensitive information. Through joint development with ISARA, Toppan hopes to equip smart cards with post-quantum public key cryptography and introduce smart card-based access authentication to quantum secure cloud technology.

- **ISARA**

  ISARA, with its knowledge and experience in cybersecurity over the years, is a global leader in crypto-agile technologies and quantum-safe security solutions that can continue to protect current computing ecosystems into the quantum age. Capitalizing on its know-how, ISARA will target the development of authentication technology using quantum-safe public key cryptosystems that can be incorporated into smart cards.

38 SK Telecom applies quantum cryptographic communication technology to IP equipment

by Lim Chang-won

https://www.ajudaily.com/view/20210406110320727

SK Telecom, a top mobile carrier in South Korea, opened the way for the wider use of its security solution by applying quantum cryptographic communication technology to corporate IP equipment such as routers

and switches. Companies with no dedicated networks can use telecom security services using quantum cryptography.

SK Telecom (SKT) and its subsidiary ID Quantique (IDQ), a Geneva-based leader in quantum-safe cryptography, have developed a quantum virtual private network (VPN) based on the quantum key distribution (QKD). VPN is a secured communications channel implemented over shared, public networks to connect remote users and machines to a private network. QKD is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics.

Quantum VPN technology combines IP equipment security technology and quantum encryption technology for enterprises, and it can be applied flexibly to various business-to-business (B2B) network structures and services, SKT said, adding it would contribute to popularizing quantum cryptographic communication technologies and improving security services for enterprises.

In the 5G era, the importance of cybersecurity in mobile communications will rise exponentially. Quantum cryptography has emerged as an essential solution for safeguarding critical information because it is impossible to copy data encoded in a quantum state. The mobile carrier has applied encryption technology using QKD to 5G networks.

"This link provides the foundation for more B2B customers to experience advanced quantum security." SKT's Innovation Suite head Ha Min-yong said in a statement on April 6. SKT would develop various methods that link QKD while upgrading QKD performance and reviewing various cryptographic methods to create a safe communication environment.

SKT is a leading member of South Korea's state project to secure technology competitiveness in quantum cryptography communication. The project involves the Korea Information Society Agency (NIA), SK Broadband and IDQ. Hanwha Systems validates security by linking a quantum cryptography communication network to virtual desktop infrastructure. Desktop virtualization separates the desktop environment and associated application software from the physical client device that is used to access it.

05 Apr 2021

39 Faster, Larger Quantum Computers Using Qubits Composed of Holes

by Karine

https://thequantumhubs.com/faster-larger-quantum-computers-using-qubits-composed-of-holes/

Strong spin-orbit interactions make hole quantum dots central to the quest for electrical spin qubit manipulation enabling fast, low-power, scalable quantum computation. Yet it is important to establish to what extent spin-orbit coupling exposes qubits to electrical noise, facilitating decoherence.

A team of researchers, taking Ge as an example, has showed that group IV gate-defined hole spin qubits generically exhibit optimal operation points, defined by the top gate electric field, at which they are both fast and long-lived: the dephasing rate vanishes to first order in the electric field noise along with all directions in space, the electron dipole spin resonance strength is maximized, while relaxation is drastically reduced at small magnetic fields.

The existence of optimal operation points is traced to group IV crystal symmetry and properties of the

Rashba spin-orbit interaction unique to spin-3/2 systems.

Their results overturn the conventional wisdom that fast operation implies reduced lifetimes and suggest group IV hole spin qubits as ideal platforms for ultra-fast, highly coherent scalable quantum computing.

40 Encryption Has Never Been More Essential – or Threatened

by will cathcart

https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/opinion-encryption-has-never-been-more-essential-or-threatened/amp

Five years ago today, WhatsApp completed our roll out of end-to-end encryption, which provides people all over the world with the ability to communicate privately and securely. This was a technical achievement decades in the making, a vision first imagined by Stanford mathematicians Whit Diffie and Martin Hellman, who in 1975 developed the underlying cryptography we rely on today.

In the past five years, WhatsApp has securely delivered over 100 trillion messages to over 2 billion users. During the height of the global pandemic lockdown, end-to-end encryption protected people's most personal thoughts when it was impossible to come together in person.

End-to-end encryption is now the way most messages are sent globally. Much as you might expect this technology to always secure our personal communications, we cannot take end-to-end encryption for granted. There remains serious pressure to take it away.

Elected officials in Europe have recently called for companies to build ways to break into their own encryption. In India, regulators have published new rules for messaging services that would undermine people's ability to have a private conversation. Brazil's Supreme Court may soon decide whether the government can shut off encrypted messaging services, in a case that started after a Facebook executive was arrested for not providing police with messages we could not access. Any of these steps could alter the course of the internet at a time when people need strong security more than ever.

Technical as encryption can be, it is really about something at the very core of how we live our lives today: Should people be able to have a private conversation when they are not together in person?

I believe the answer must be yes. People speak to each other privately in person all the time. As human beings we're wired to assume that when we're talking to someone face to face, our conversation is private. We shouldn't give that up. The lessons of the past five years make it absolutely clear that technology companies and governments must prioritize private and secure communication.

End-to-end encryption helps solve a fundamental problem of how the internet evolved. While the WhatsApp you see on your phone or desktop looks simple, it's the product of decades of investment. Chats and calls are automatically routed via a global network of data centers and traverse cell towers and mobile networks built by carriers using hardware of various designs.

These real-time networks provide enormous benefits, but only if we can overcome the security challenges of relying on this patchwork of technology. The more interconnected we are, the more corporations, criminals, and authoritarian governments can find new ways to access what we write and say.

The stakes are not just a matter of personal, financial, or reputational risk for the few. Given the reliance on global communication by nearly every economy on the planet, how technology is built impacts people everywhere in different ways. In many parts of the world, people live in fear that the real-time networks they rely on will be used by authoritarian governments to oppress them.

Sadly, the same technology that makes it easier for dissidents to speak up also makes it easier for dictators to crack down. Saudi Arabia and many other countries rely on commercial digital espionage services to track, jail, and even kill journalists, including outside their own nation. They are receiving help from unaccountable foreign companies selling hacking services to governments on multiple continents without any regard for the consequences to people's human rights.

And of course one country has chosen to build its internet in a way that's designed to eliminate privacy. The leading messaging service in China relies on automatic filters to censor conversations. Fearful of their phones, people try workarounds by chatting with emojis, GIFs, and innuendo.

Given the global nature of the internet, the decisions some countries make affect us all. Foreign powers have already stolen personal data tied to half of all Americans. In the last six months, we've seen devastating attacks on the servers of major companies and governments that continue to use unsecure email. The consequences of these attacks can play out over the course of a lifetime.

For most of human history, we have felt free to confide in one another about our families, our work, our hopes, and our fears. That sense of freedom comes from the knowledge that once our words left our lips, they weren't recorded.

But if nothing online is private, and every conversation today is online, then no conversation is private. That would leave us with two choices: Either we communicate face-to-face, or we surrender any expectation that we're alone.

That's not a realistic way to live. We carry and check our phones from the moment we wake up to the moment we go to sleep. In an emergency, your phone is probably one of the first things you'd grab.

Just because we have vastly improved the technology that lets us communicate with people far away doesn't mean our privacy should go away. Machines today might make it possible for someone else to see and hear what we're doing and what we've said, but that doesn't mean they should.

That's what makes end-to-end encryption so valuable. As complex and advanced as it is, the idea behind it is thousands of years old. Early cryptography made it possible for people to communicate securely, but only if they had already exchanged a secret "key" ahead of time.

But that's not practical in today's world. Exchanging secret "keys" with everyone you know ahead of time and tracking those keys yourself would be tedious at best. Modern technology has made this seamless. The end-to-end encryption WhatsApp uses automatically exchanges the "key" directly on the sender's and recipient's physical devices and nowhere else. Every single message has its own separate lock and key.

It's no surprise, then, that many technology companies have added end-to-end encryption, and that since the pandemic started, several more have scrambled to upgrade their systems to protect the growing volume of critical communication happening digitally.

Knowing that you can communicate confidentially beyond the sound of your voice matters. It makes it possible for doctors to see patients remotely, helps militaries protect operational secrets, supports people building businesses, and protects journalists bringing important information to light. It also makes it possible for us to have the most private conversations with the people we care about, confident that we can speak our mind to the people closest to us without fear that someone is listening in.

End-to-end encryption locks tech companies out of particularly sensitive information, and for good reason. In 2019, the Justice Department filed charges in a case where people connected to Saudi Arabia were allegedly spying on dissidents using internal access tools. With end-to-end encryption, even employees do not have the ability to access private messages, for any purpose. This has caused frustration with

governments who want tech companies to provide private messages under legal process.

Some governments are honestly trying to fight crime and looking to the dramatic increase in technology in our lives as a potential source of new evidence. Their criticism is that end-to-end encryption makes it harder for law enforcement to find evidence of a crime, and harder for companies to monitor people's calls and messages to refer to law enforcement. But this is looking at a problem in isolation. It was never possible or easy to access most people's private conversations when they were happening physically instead of digitally. We should not assume that just because technology makes something easier to do, we should do it.

We intuitively understand this when we think of physical spaces. Some of the most tragic crimes happen in the privacy of people's homes. That doesn't mean we would let the government put a surveillance camera in every house with a remote-controlled on/off switch. For the same reason, we should not build a means to silently monitor billions of private conversations just because we could.

The reason it was technically possible to wiretap a phone conversation was because listening in was as simple as physically placing clips on a wire. We've all seen that scene in the movie. But a digital version of this capability is far too dangerous. Building a way to see one message makes it possible to see them all. And with the right access and sophistication, a hacker or foreign adversary could do something that has never been possible in human history: steal every conversation at once across billions of people. That's far too great a risk.

There are still ways of preventing or addressing harm without breaking encryption. WhatsApp, for example, can and does provide unencrypted account information to authorities, including metadata, to assist investigations when required by law. We made over 400,000 reports to child safety authorities last year and people have been prosecuted as a consequence.

We respond quickly when people report illegal behavior. And by employing sophisticated techniques to analyze metadata, user reports, and other unencrypted information, we ban millions of dangerous accounts every year. We're constantly getting better at our efforts.

We should also consider all the other digital information governments have access to and not look at an individual app in a silo. Even in a world where private conversations are secure, law enforcement has access to a dramatically increasing volume of information. The digital trails we all leave are so vast that law enforcement can even use warrants to figure out everyone who was in a certain place at a certain time.

Breaking encryption would make us less safe for a simple reason: Every time you build a weakness into a security system, you create a magnet for intruders. This has been tried in the past and failed. An intentional weakness built into routing software provided by Juniper Networks, purportedly to advantage the US government, was later discovered and exploited by foreign powers.

Governments are demanding companies build a special key to access private messages. But once the key to your messages is created, can you guarantee it won't be copied? Are you confident that a hacker or a foreign spy won't steal it, or that your government won't lose it? Once that key opens a back door, how do you know a criminal won't sneak inside? And even if a government keeps the key safe, should we trust them not to mishandle the messages we send?

In recent years, even government agencies have fallen victim repeatedly to infiltration. In 2015 hackers from the Chinese military compromised the information of more than 22 million public servants. The sensitive data collected for background checks could be used to embarrass or blackmail US government officials. In June a data vendor for law enforcement officials, so-called "BlueLeaks," spilled personal data of American citizens dating back to 1996, including people who never committed any crime.

Given the stakes, governments should be demanding that technology companies provide people with the strongest security possible.

In many ways, the pandemic accelerated the reality that in the years to come, our lives, livelihoods, and safety will rely on technology even more than they do today. Will we be able to have a private conversation, or will someone always be listening in? The choice we make will have lasting consequences for future generations.

In the last century, Hannah Arendt helped us understand totalitarianism as the elimination of privacy by the state. I fear that if we abandon or weaken the tools that preserve our privacy and security, censorship will come not from above, but from within.

Imagine if your government, or a foreign one, could see every transaction you made, or if your boss could see every text message you wrote or photo you sent. What if your friends could see every question you asked your doctor?

That's the greatest risk of all: No matter how well-meaning the motivation, surrendering our privacy would paralyze us. The power of technology is that it lets us connect at extraordinary speed and scale and democratizes information better than anything ever invented. But if we choose to erode our privacy and security, it will do the opposite. Instead of sharing our ideas, it will shut them down. Instead of bringing us closer together, it will keep us apart. Instead of giving everyone in the world a voice, it will silence us.

41 What is homomorphic encryption, and why should you care?

by Jack Gold

https://www.idginsiderpro.com/article/3613551/what-is-homomorphic-encryption-and-why-should-you-care.html

The amount of data captured by enterprises continues to grow astronomically. Indeed, data warehouse are filled with huge amounts of confidential data like personally identifiable information, company financial records, Intellectual Property (IP), corporate strategic documents, etc. Common practice is to encrypt that data while in storage and during transport, but that is not always a guarantee that the data is safe from exposure. It does offer a reasonable level of protection from less sophisticated attackers, as capturing the encrypted data and running a massive computing system that tries to break that encryption through brute force operations is difficult. The brute force method is very inefficient and mostly available only to special sophisticated operations (e.g., state sponsored massively large resourced systems). It also isn't very effective at extracting data in volume as it's a time consuming process that can't keep up with real time data creation. But there is a loop hole many hackers have exploited to obtain potentially large volumes of encrypted data that is available to them unencrypted.

The challenge with the current state of data computation is that the only way encrypted data can be processed in a typical computing system, either on-premise or in the cloud data center, is by first decrypting that data, placing it in local memory and then running the computing application against it. Once the operation is completed, the data may then again be encrypted before going back to storage. This process also requires that the computing system has the appropriate keys for doing the decryption. This presents a serious problem since once that data is decrypted during processing it is available for attack and exfiltration from the computing system by different exploits and system anomalies. This is a primary target of many hackers who are able to extract volumes of data by infiltrating the compute stack and continuously retrieving unencrypted data from operating memory. Or even easier is for hackers to

just steal the decryption keys and have immediate access to all the data through decryption on their own systems.

What's needed is a better way to work with sensitive data, and in fact, almost all data is becoming sensitive as new data regulations become operative, like GDPR, HIPPA, and various other data protection regulations. Further, there are many classes of data analysis, especially in AI/ML processes, that require sensitive data to be provided from many different sources (e.g., aggregated healthcare data, individual financial records), but that also needs to remain confidential. In an ideal world, compute operations should be able to be done without ever decrypting the data, thus preventing exposure of any sensitive data to hackers, even if they were able to gain access to the processing or storage elements. Enter homomorphic encryption and computing.

What is homomorphic computing?

Homomorphic computing operates on the principal that all data must remain encrypted through all operations within the processing system. While it's possible to do so in current systems, the throughput for operations could be slowed by a factor of 10 orders of magnitude or more, making it unacceptable in large scale operations. That means that a new generation of computing system must be designed that can process the encrypted data streams, and do so in a way that doesn't significantly slow down the compute cycle. Building a system to execute general purpose programs on encrypted data requires a totally new platform in both hardware and software, and it's not a simple thing to do.

Doing it a massive scale

A true homomorphic processing system, in order to be equivalent in execution speeds to current 64-bit processors running against unencrypted data, would have to have a massive compute width of up to 1024 bits! Further, since this compute is being done in a highly parallel fashion, the interconnections must be equally as wide and be extremely fast. And of course memory needs to be designed to compliment this wide and fast path. And finally the software algorithms need to be adapted to this new environment. While we currently have many parallel processing systems, like GPUs and AI/ML accelerators, the latency in stringing a large number of these systems together and interconnecting them would make the compute cycle unacceptable. Therefore, current processors are not a good solution for at-scale homomorphic computing implementations. Further, encryption algorithms need to be redesigned to take advantage of this massive parallelism. As a further complication, working on encrypted data makes for unacceptable "noise" that can create errors. With larger word sizes of 1K bits, the amount of noise introduced in the computing cycle is reduced and makes processing much more accurate.

Moving towards productization and standards

Making this real will take massive engineering efforts as well as necessitating the creation of standards. To make this a reality, Intel is partnering with Defense Advanced Research Projects Agency (DARPA) in its Data Protection in Virtual Environments (DPRIVE) program. As part of the program Intel expects to develop an accelerator for fully homomorphic encryption. To work on the needed software infrastructure required, Microsoft is also a program partner and leading the commercial adoption by testing it in its Microsoft Azure and the Microsoft JEDI cloud environments, with the US government participation.

As part of DPRIVE, Intel will design an application-specific integrated circuit (ASIC) accelerator for fully homomorphic encryption, potentially reducing processing time by five orders of magnitude over

current CPU implementations. And Microsoft will utilize its expertise in cloud infrastructure, software stacks and fully homomorphic encryption, to potentially reduce processing time by two orders of magnitude, and to accelerate the commercialization of this technology when ready. Once accomplished, homomorphic encryption will go a long way towards enabling free data sharing and collaboration of sensitive data, while promoting privacy throughout the data life cycle. Beyond the development of the core technologies needed, Intel and Microsoft will work with international standards bodies to develop international standards, a necessary step to guarantee wide adoption.

But don't expect commercial systems soon

There will be multiple phases to the DPRIVE program and major milestones to hit along the way. But the program itself is 42 months long and ends in 2024, and it is likely to take another 1-2 years beyond the program for commercialization to take place. That means homomorphic encryption systems probably won't be available until 2025/26, and perhaps later. Still, the potential benefits of homomorphic, if successfully implemented, will dramatically change the way sensitive data can be processes and confidential computing can be implemented.

Bottom line: Homomorphic encryption is currently an academic exercise and an advanced engineering project. But it presents a major advancement in securing sensitive data from exposure. With the backing of major players like DARPA, Intel and Microsoft, it is likely to become a reality, but probably not for 5 years. Once deployed at scale, I expect to see a major shift for many industries that need to do a better job of protecting their data from exposure and hacking. Enterprises should be monitoring this technology for the next few years to gauge i

42 UK-based Quantum Motion Researchers Report They Have Blueprint for Scalable Future in Quantum Computing

by Matt Swayne

https://thequantumdaily.com/2021/04/05/uk-based-quantum-motion-researchers-report-they-have-blueprint-for-scalable-future-in-quantum-computing/

Quantum Motion, a UK-based quantum computing startup led by academics from UCL and Oxford University, has made an advance that the researchers say improves the viability and production of quantum computers, according to a company statement. Quantum Motion has been able to demonstrate state-of-the-art quantum capabilities using industrial-grade silicon chips, helping to set a blueprint for how quantum chips can be manufactured at scale using existing manufacturing processes. The discovery has been peer reviewed in the scientific journal PRX Quantum.

According to the statement: the discovery changes the dynamics in the development of quantum computing, showing that it is possible to build devices at scale using established processes and fabrication plants. This contrasts with other industry approaches that are looking at totally new manufacturing processes or even newly discovered particles. This potentially makes quantum computing development quicker and more cost effective.

A quantum computer harnesses some of the deepest laws of physics, normally seen only at the atomic and subatomic level, giving it unique powers to model the natural world. Quantum computers could be more powerful than today's super computers and capable of performing complex calculations that are otherwise

practically impossible. While the applications of quantum computing differ from traditional computers, they will enable us to be more accurate and faster in hugely challenging areas such as drug development and tackling climate change, as well as more everyday problems that have huge numbers of variables – just as in nature – such as transport and logistics.

"We're hacking the process of creating qubits, so the same kind of technology that makes the chip in a smartphone can be used to build quantum computers," said John Morton, Professor of Nanoelectronics at UCL and co-founder of Quantum Motion. "It has taken 70 years for transistor development to reach where we are today in computing and we can't spend another 70 years trying to invent new manufacturing processes to build quantum computers. We need millions of qubits and an ultra-scalable architecture for building them, our discovery gives us the blueprint to shortcut our way to industrial scale quantum chip production."

The peer reviewed paper demonstrates that Quantum Motion has been able to isolate and measure the quantum state of a single electron for a period of nine seconds on a CMOS chip. The chips were manufactured at CEA Leti, a large microelectronics facility in Grenoble, France. Qubits, the building blocks of quantum computers, are often realised using exotic technologies such as superconductors or individually trapped atoms. The big breakthrough is the proof that it is possible to create a stable qubit on a standard silicon chip, like those found in any smartphone, rather than one specially created in a lab environment. Combined this creates the potential for stable and scalable quantum computing.

The experiments were performed by Virginia Ciriano Tejel, a PhD student working in a low-temperature laboratory at UCL, and co-workers. During operation, the chips are kept in a refrigerated state, cooled to a fraction of a degree above absolute zero (-273 degrees Celsius).

Virginia described the eureka moment, "Every physics student learns in textbooks that electrons behave like tiny magnets with weird quantum properties, but nothing prepares you for the feeling of wonder in the lab, being able to watch this 'spin' of a single electron with your own eyes, sometimes pointing up, sometimes down. It's thrilling to be a scientist trying to understand the world and at the same time be part of the development of quantum computers."

Quantum Motion was founded in 2017 and has raised £8million in series A funding, led by INKEF capital, a Dutch based venture capital company. The round was supported by new investors Octopus Ventures and the National Security Strategic Investment Fund (NSSIF) as well as existing investors Oxford Sciences Innovation, Parkwalk Advisors and IP Group plc.

03 Apr 2021

43 IBM bets homomorphic encryption is ready to deliver stronger data security for early adopters

by Chris O'Brien

https://venturebeat.com/2021/04/03/ibm-bets-homomorphic-encryption-is-ready-to-deliver-stronger-data-security-for-early-adopters/

The topics of security and data have become almost inseparable as enterprises move more workloads to the cloud. But unlocking new uses for that data, particularly driving richer AI and machine learning, will require next-generation security.

To that end, companies have been developing confidential computing to allow data to remain encrypted while it is being processed. But as a complement to that, a security process known as fully homomorphic encryption is now on the verge of making its way out of the labs and into the hands of early adopters after a long gestation period.

Researchers like homomorphic encryption because it provides a certain type of security that can follow the data throughout its journey across systems. In contrast, confidential computing tends to be more reliant upon special hardware that can be powerful but is also limiting in some respects.

Companies such as Microsoft and Intel have been big proponents of homomorphic encryption. Last December, IBM made a splash when it released its first homomorphic encryption services. That package included educational material, support, and prototyping environments for companies that want to experiment.

In a recent media presentation on the future of cryptography, IBM director of strategy and emerging technology Eric Maass explained why the company is so bullish on "fully homomorphic encryption" (FHE).

"FHE is a unique form of encryption, and it's going to allow us to compute upon data that's still in an encrypted state," Maass said.

Evolving encryption

First, some context. There are three general categories of encryption. The two classic ones are encryption for when **data is at rest** or stored and then "**data in transit**" that protects the confidentiality of data as it's being transmitted over a network.

The third one is the piece that has been missing: the ability to compute on that **data while it's still encrypted**.

That last one is key to unlocking all sorts of new use cases. That's because until now, for someone to process that data, it would have to be unencrypted, which creates a window of vulnerability. That makes companies reluctant to share highly sensitive data involving finance or health.

"With FHE, the ability to actually keep the data encrypted and never exposing it during the computation process, this has been somewhat akin to a missing leg in a three-legged crypto stool," Maass said. "We've had the ability to encrypt the data at rest and in transit, but we have not historically had the ability to keep the data encrypted while it's being utilized."

With FHE, the data can remain encrypted while being used by an application. Imagine, for instance, a navigation app on a phone that can give directions without actually being able to see any personal information or location.

Companies are potentially interested in FHE because it would allow them to apply AI to data, such as from finance and health, while being able to promise users that the company has no way to actually view or access the underlying data.

While the concept of homomorphic encryption has been of interest for decades, the problem is that FHE has taken a huge amount of compute power, so much so that it has been too expensive to be practicable.

But researchers have made big advances in recent years.

For instance, Maass noted that in 2011, it took 30 minutes to process a single bit using FHE. By 2015, researchers could compare two entire human genomes using FHE in less than an hour.

"IBM has been working on FHE for more than a decade, and we're finally reaching an apex where we

believe this is ready for clients to begin adopting in a more widespread manner," Maass said. "And that becomes the next challenge: widespread adoption. There are currently very few organizations here that have the skills and expertise to use FHE."

FHE is ready for its close-up

During the presentation, AI security group manager Omri Soceanu ran an FHE simulation involving health data being transferred to a hospital. In this scenario, an AI algorithm was used to analyze DNA for genetic issues that may reveal risks for prior medical conditions.

That patient data would typically have to be decrypted first, which could raise both regulatory and privacy issues. But with FHE, it remains encrypted, thus avoiding those issues. In this case, the data is sent encrypted and remains so while being analyzed, and the results are also returned in an encrypted state.

It's important to note that this system was put in place using just a dozen lines of code, a big reduction from the hundreds of lines of code that have been required until recently. By reducing that complexity, IBM wants to make FHE more accessible to teams that don't necessarily have cryptography expertise.

Finally, Soceanu explained that the simulation was completed in .069 seconds. Just five years ago, the same simulation took a few hours, he said.

"Working on FHE, we wanted to allow our customers to take advantage of all the benefits of working in the cloud while adhering to different privacy regulations and concerns," he said. "What only a few years ago was only theoretically possible is becoming a reality. Our goal is to make this transition as seamless as possible, improving performance and allowing data scientists and developers, without any crypto skills, a frictionless move to analytics over encrypted data."

Next steps

To accelerate that development, IBM Research has released open source toolkits, while IBM Security launched its first commercial FHE service in December.

"This is aimed at helping our clients start to begin to prototype and experiment with fully homomorphic encryption with two primary goals," Maass said. "First, getting our clients educated on how to build FHE-enabled applications and then giving them the tools and hosting environments in order to run those types of applications."

Maass said in the near term, IBM envisions FHE being attractive to highly regulated industries, such as financial services and health care.

"They have both the need to unlock the value of that data, but also face extreme pressures to secure and preserve the privacy of the data that they're computing upon," he said.

But he expects that over time a wider range of businesses will benefit from FHE. Many sectors want to improve their use of data, which is becoming a competitive differentiator. That includes using FHE to help drive new forms of collaboration and monetization. As this happens, IBM hopes these new security models will drive wider enterprise adoption of hybrid cloud platforms.

The company sees a day, for instance, when due diligence for mergers and acquisitions is done online without violating the privacy of shareholders and when airlines, hotels, and restaurants use FHE to offer packages and promotions without giving their partners access to details of closely held customer datasets.

"FHE will allow us to secure that type of collaboration, extracting the value of the data while still preserving the privacy of it," Maass concluded.

02 Apr 2021

44 Canada's Defense Strategy Falls Behind in the Quantum Age

by Tina Dekker, Florian Martin-Bariteau

https://www.lawfareblog.com/canadas-defense-strategy-falls-behind-quantum-age?utm_medium=email&_hsmi=123973517&_hsenc=p2ANqtz-81zit13SRDpD3HOa6wDLKFDzrH-FZOcSdBSG2Uo4JQ225vL88c4nsL5_vs2QvVtbHxFR_hDK1yBwwTPIqNXZ4iDDFtAg&utm_content=123973517&utm_source=hs_email

Governments around the world are in a race against time to both leverage the opportunities and mitigate the risks of the next quantum technological revolution. Quantum materials will underpin next-generation electronics and equipment for the military environment, while quantum communication technologies offer ultra-secure communication channels for sensitive information. Quantum computing, perhaps the most disruptive technology, promises improved simulation and modeling capabilities and powerful artificial intelligence. But this computational advantage also poses cyber and national security risks to existing cybersecurity infrastructure, which is secured using the types of mathematical problems that quantum computers will be capable of solving. Given these risks, governments need to prepare a "quantum firewall" – and fast.

Many countries are investing in the quantum ecosystem through various national and international programs and have developed national and departmental quantum strategies. China, for example, is deeply committed to leverage quantum advances, including in the quantum arms race. In 2018, the United States launched its national strategy through a major quantum initiative and has published more than 40 reports and strategies to further the country's quantum ecosystem, including about the opportunities for defense and risks for national security. Similarly, in 2020, the United Kingdom released a strategic vision that provides an outlook for the next decade, as well as a detailed report on quantum information processing considerations for defense and security.

By comparison, Canada is missing in action and lagging behind – despite its global leadership in quantum research, driven by a rich university-led ecosystem. That's not to say that Canada has fully overlooked quantum. The federal government published two innovation reports from 2014 and 2016 mentioning quantum innovation as a priority in Canada, and the 2018 National Cyber Security Strategy similarly acknowledges the need to have "quantum-resistant solutions." Canada's first federal department quantum "strategy" was finally released on Jan. 18 by the Department of National Defence and the Canadian Armed Forces – the so-called "Defence Team." Yet this new report falls far short of delivering a meaningful strategy, even just for defense. It fails to address important questions about the potential impacts of quantum technologies on Canada's national defense and security, and on society more generally – and it highlights Canada's failure to deliver a comprehensive vision in the growing quantum sector.

Many technical hurdles must be overcome to make quantum capabilities available, but that's no reason for Canada to dawdle. Quantum technologies might be developed within the next five to 20 years, or even sooner. And when they arrive, their use will not be confined within restricted facilities – instead, they will be accessible through publicly available cloud services connected to various quantum hardware implementations. So while the quantum threat might seem distant, a response is required right now. In the global arms race, it might already be too late.

Even though new cybersecurity standards have been in development, the implementation of new standards is historically a slow process. Malicious actors can already retrieve encrypted information to later be decrypted using quantum computing methods when those methods become available. More than any other technology revolution, the everyday quantum reality requires foresight and readiness before its advent.

The Defence Team's announcement claims that its Quantum Science and Technology Strategy will "advanc[e] Canada's defence, safety and security interests in the emerging field of quantum science" and help "to take advantage of cutting-edge science and adapt to quantum innovation." This is, however, quite a generous title and aim for a document that focuses on research and development (R&D), investments, and operational partnerships for quantum sensing technology. Indeed, authored by the assistant deputy minister heading Defence Research and Development Canada (DRDC), the report is really a belated R&D road map for the agency.

Yet this road map is an important first step in providing Canada with necessary leadership in quantum technology R&D to be ready for what's to come – although, admittedly, nobody really knows what is to come. Recognizing Canada's strong leadership in quantum technology R&D, DRDC notes the increasing global competition to transition quantum technologies to market launch and highlights Canada's need to be defensively prepared.

The first goal of DRDC's "strategic" approach is to transition quantum sensing technologies from the lab into robust, fieldable prototypes. Quantum sensors promise new or improved, highly sensitive detection of physical phenomena and objects that can be used, for example, to detect magnetic fields or stealthcraft. In parallel to R&D efforts, DRDC plans to assess threats and vulnerabilities, as well as to develop security and countermeasures against those threats. However, while quite comprehensive on prototyping quantum sensor technology, the road map inexplicably leaves out the three other key areas of quantum technology: communications, materials and computing. Each of these topics deserves recognition but is mentioned only in passing, if at all.

It's not just unfortunate but concerning that the government doesn't consider such technologies as a priority – or even an opportunity – for the Defence Team. Quantum materials could bring to the battlefield next-generation microelectronics with improved capabilities, while quantum communication technologies could help secure communication in sensitive areas, as well as global positioning. DRDC also disregards the myriad applications proposed for quantum computing in simulation, optimization, and artificial intelligence that may contribute to defense efforts. For example, quantum computers could be used for large-scale military deployment simulations, the development of novel materials, and to leverage (or counter) sophisticated artificial intelligence systems.

The road map also aims at fostering partnerships interdepartmentally, domestically with universities and industry, and internationally to advance quantum technology development for defence at both national and international levels. The report vaguely suggests that these partnerships can be leveraged to develop quantum technologies for defense, security, and public safety purposes but doesn't offer any concrete examples, proposals or action plans. As the road map notes, quantum science and technology innovation has been a national "priority" since 2014 – so why are these interdepartmental relationships being proposed more than five years later?

Overall, the report can be summarized as a commitment to work with the government and industry to further quantum research and innovation – which makes sense for a road map authored by defense R&D agencies. The road map highlights DRDC's aim to improve the department's capacity to remain apprised of defense and security impacts by emerging quantum technologies. Noting that labor shortages

of quantum-trained personnel are likely, the road map calls for the development of a quantum-trained workforce and sustained R&D.

The scant 15-page strategy leaves readers with the feeling that something is missing. The report does not offer any policy analysis of the impact of quantum technologies on Canadian society. There is no security framework to protect the Canadian quantum sector and to protect the country from potential quantum-enabled threats. These omissions in the Defence Team's quantum strategy could be understandable if the report was published as a focused perspective following a more general national quantum strategy. However, no such national quantum strategy exists – at least not publicly.

Definitive and decisive action is required to set Canada on the path to establish and sustain leadership in the global quantum sector. Canada will not remain relevant in the quantum race by supporting R&D from the sidelines with half-baked promises to prioritize Canada's quantum ecosystem.

This initial road map can only whet Canadians' expectations for a more comprehensive strategy. So what would a true defense quantum strategy look like? It would need to be released by the minister of national defence – and involve all branches of the Defence Team, notably Canada's cryptologic agency, the Communications Security Establishment. It would highlight the ethical, warfare, and national security dimension of quantum technology. Such a strategy should be developed, at least in part, in collaboration with the minister of public safety and the minister of foreign affairs, who share oversight over part of the intelligence and national security apparatus. The report obviously comes up short in this dimension, which is concerning not just for the Defence Team but also for the whole government and country.

A strategy would also need to reflect on how quantum technologies – of all types, not just sensor technology – will impact Canada's security and defense, and explain how the Defence Team intends to build a "quantum firewall" to address the potential negative impacts of defense-themed quantum technologies on society, foster the ethical development of quantum technologies, and lead the global community in setting the standard for a safe ecosystem in which quantum technologies can be applied. It would also need to engage with the policy and regulatory needs – at both the national and international levels – for Canada and the world to be quantum-ready. While there is some nebulous guidance on post-quantum readiness to federal agencies from the Canadian Centre for Cyber Security, a strategy should discuss challenges and opportunities for the cryptologic community, and how to rethink data governance and security for the quantum age. For example, it could make sense to consider classifying some quantum technologies under the military, dual-use, or strategic goods frameworks to control their development, export, commercialization and use. Use of these frameworks to regulate cryptographic tools was probably an error, but they could be useful concerning quantum technologies.

Canada needs a strategy along these lines both to ensure Canadians that the country takes the impact of quantum technologies seriously and to signal the country's presence in the global quantum sector. It is not enough to say that Canada has a thriving quantum R&D system, as R&D is only one aspect of the overall national and global quantum ecosystem – even more so given Canada's declining R&D investment in recent years.

Hopefully this first Canadian government report is not the last and, instead, marks the beginning of a strong government initiative planned to strengthen Canada's relevance in the quantum sector. Many important questions about the impact of quantum technologies on Canadian society remain. How will Canada support its quantum ecosystem, and build and maintain a quantum-trained workforce? What about building nationally shared quantum computing capabilities? What about incentivizing Canadian's quantum intellectual property? What are the potential ethical impacts of quantum technologies on society, and what are the opportunities for responsible quantum leadership? How will Canada address the security

threats posed by quantum technologies to national security and private enterprises? What about preparing Canada's policy framework to protect industries, infrastructure and citizens.

There are so many questions and so few answers – especially in the Canadian context. It's time for the Canadian government to publish a strategy and fund transdisciplinary research to prepare the country for what's to come. Government and funding agencies need to support not just corporate R&D but also universities and start-ups. Current leadership lies with a few researchers who have built bridges within Canada's thriving quantum community with initiatives such as Quantum-Safe Canada. It's now time for the government to step in and provide funding – and leadership – to carry these initiatives further.

The Canadian government appears to be floundering while other countries drive the quantum market forward. If every other country can develop and publish a national strategy, why can't Canada?

01 Apr 2021

45 NIST has completed the review of the second-round candidates in NIST's lightweight cryptography standardization process

by Michael Roza

https://circle.cloudsecurityalliance.org/community-home1/digestviewer/viewthread?MessageKey=227e711c-d787-4483-9bfb-68551ae4dddf&CommunityKey=1852507a-d005-4624-9ef7-a469e73aee07&tab=digestviewer#bm227e711c-d787-4483-9bfb-68551ae4dddf

NIST has completed the review of the **second-round candidates in NIST's lightweight cryptography standardization** process. After careful consideration, the ten finalists moving forward to the final round are:

- ASCON
- Elephant
- GIFT-COFB
- Grain128-AEAD
- ISAP
- Photon-Beetle
- Romulus
- Sparkle
- TinyJambu
- Xoodyak

Selecting the finalists was a challenge. In the upcoming weeks, NIST will publish a detailed description of the decision process and rationale for selection. The report will be available from the Lightweight Cryptography (LWC) Project Page – Round 2 Candidates – Lightweight Cryptography

NIST thanks the designers of the second-round candidates and those who have contributed to the selection process by providing security and performance analysis of the candidates. NIST hopes that the submission teams of candidates that were not selected to advance will continue to participate in the evaluation of the finalists along with the cryptographic community at large.

The final round of the standardization process is expected to last approximately 12 months. NIST will give the finalist submission teams the opportunity to provide updated specifications and implementations. Further guidelines on the tweak proposals will be provided in the upcoming days.

46 Quantum computer has the edge for NP verification

https://physicsworld.com/a/quantum-computer-has-the-edge-for-np-verification/

One of the main goals in quantum computing is to experimentally demonstrate that a quantum machine can perform some computational task faster than a classical one. A team of researchers based in France and the UK has now done just that using a simple quantum photonics experimental set-up. Their work shows that it is possible for a quantum computer to verify solutions to problems classified as NP-complete using a so-called interactive proof protocol and only minimal, unverified information about the solution.

The work is among several recent milestones in demonstrating quantum advantage. In 2019, Google claimed to be the first to the finish line with their 53 programmable superconducting qubit (quantum bit) set-up. More recently, a team in China announced that they had successfully performed‘ ‘boson sampling”, a task known to be hard for a classical computer. Unlike these previous results, however, the new research, which is published in Nature Communications, not only demonstrates quantum advantage but also promises to be useful in applications like secure quantum cloud computing.

NP verification

Although NP-complete problems are hard to solve efficiently, once solutions are found, they can be verified trivially. The challenge that the team at CNRS (the French National Centre for Scientific Research) and the University of Edinburgh focused on occupies a middle ground between the two: verifying the solution to an NP-complete problem when provided with only a part of that solution.

When the size of the message containing the partial solution, or proof, is fixed, it can be shown that a classical protocol for verifying the solution will take an amount of time that scales exponentially with the size of the message. For the quantum protocol, in contrast, the scaling is polynomial. This means that for large message sizes, a quantum computer would take minutes to verify the solution while a classical one could take years.

The algorithm the researchers use to demonstrate this is known as an interactive proof protocol. Here, one component of the experimental set-up acts as a “prover”, using coherent light pulses to send partial solutions to the NP-complete problem in the form of a quantum state. The second component fills the role of the “verifier”, deciding with high accuracy whether the solution is correct based on the limited information given. When certain bounds are placed on the expected accuracy of the verifier, as well as the protocol’s speed and efficiency in terms of the amount of information that can be communicated throughout the interactions, it is possible to demonstrate that the quantum algorithm far outperforms any classical attempts at doing the same.

Quantum cloud computing

By showing that a quantum algorithm can verify solutions to NP-complete problems efficiently, the result could allow for new applications in secure remote quantum computing. A client with a rudimentary quantum machine could, for example, verify information they receive from a powerful quantum server without ever having access to the full solution. Such proof systems could then contribute to protocols like secure identification, authentication or even blockchain in a future quantum Internet. "In the current era of increasing focus on data privacy and secure computing, our demonstration provides yet another compelling piece of evidence that quantum computers can outperform their classical counterparts in achieving secure solutions," adds Niraj Kumar, an Edinburgh researcher and a co-author on the paper.