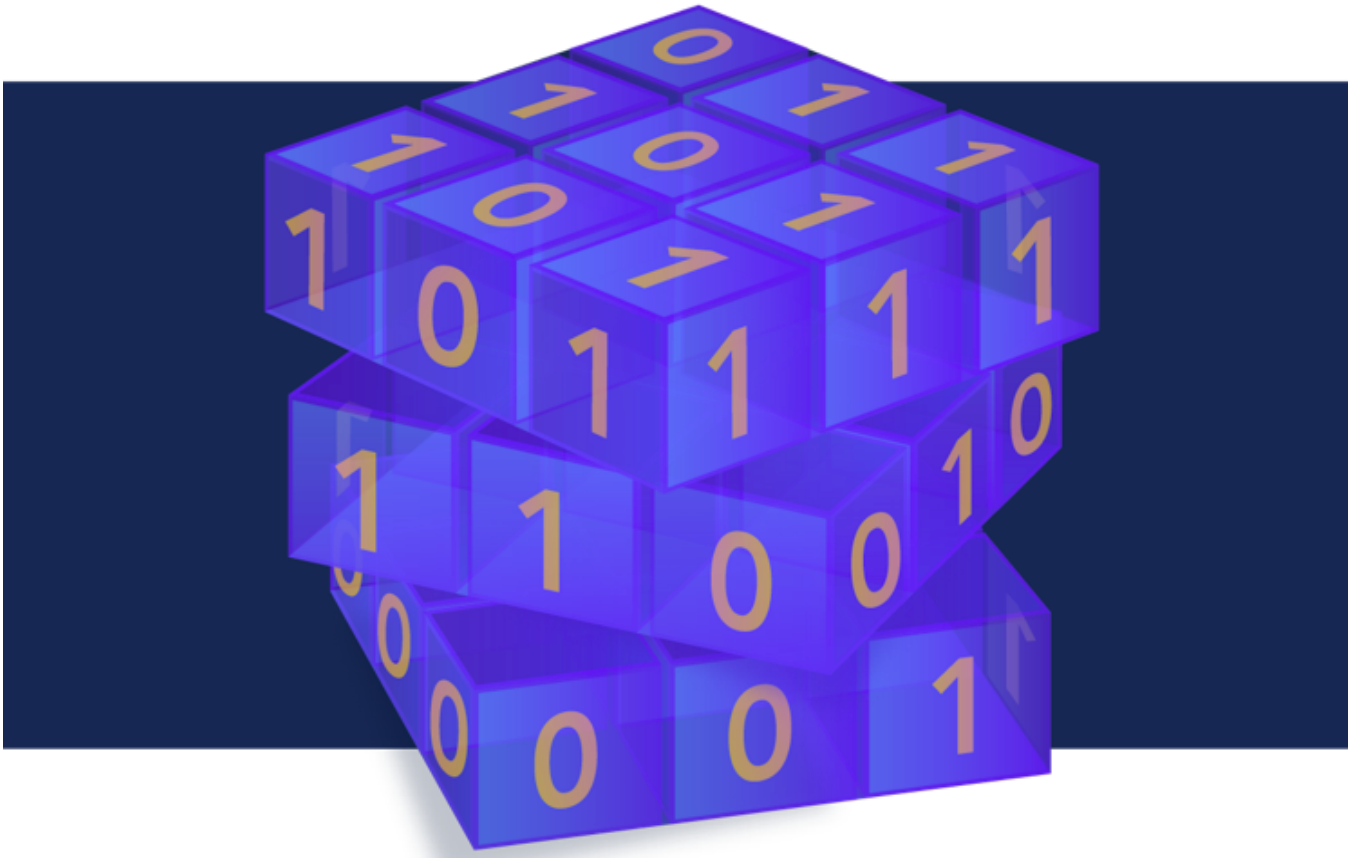
Cloud Security Alliance
Crypto News
July 1, 2021

Crypto News

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

July 1st, 2021



Contents

July, 1st, 2021

1 A New form of the Crypto News

SEATTLE, WA – July, 1st, 2021. The Cloud Security Alliance (CSA), the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment, today released the Crypto News compiled by Dhananjoy Dey member of the CSA Quantum-Safe Security Working Group (QSS WG). The CSA QSS WG was formed to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting their networks and their data. Individuals interested in joining the working group and participating in future research can do so by visiting the page at https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/ or the LinkedIn account.

The Crypto News is intended to provide an overview of the latest news in quantum-safe security and more broadly in security.

About Cloud Security Alliance. The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem. For further information, visit us at https://cloudsecurityalliance.org/, and follow us on Twitter @cloudsa.

2 New gate optimization strategy could boost efficiency in trapped-ion quantum computers

by Oliver Stockdale

https://physicsworld.com/a/new-gate-optimization-strategy-could-boost-efficiency-in-trapped-ion-quantum-computers/

Physicists at the University of Maryland, US and the quantum computing firm IonQ have found a new way to make a central operation in quantum computing more efficient. By slashing the laser power required to perform a so-called two-qubit gate, the collaborators showed that they could speed up the gate's operation, thereby boosting the performance of their trapped-ion quantum computer.

The building blocks of a quantum computer are qubits – quantum bits that can be in any superposition of two states. In this work, the researchers used ions as their qubits. Rapidly oscillating electric fields trap the ions in a chain, making it possible to perform computational operations by shining laser light on one or more ions.

Two-qubit entangling gates

These computational operations generally divide into two types: single-qubit gates and two-qubit gates. While single-qubit gates are relatively simple to perform and pose no significant challenges, two-qubit gates cost significant time and power. That has consequences for the overall efficiency of the quantum computer, says Norbert Linke, a fellow of Maryland's Joint Quantum Institute (JQI) and a co-author of the current study. "The performance of two-qubit entangling gates typically limits the overall system since they require the most calibration time and introduce the most error," Linke explains. "Improving these gates is therefore crucial to boost the performance and eventually scale up these systems."

Ideally, gate operations would be fast, use minimal laser power, and leave the qubit in the desired state with no errors (maximum fidelity). In the real world, errors in two-qubit entangling gates come from having imperfect control over experimental parameters such as the frequency of the laser and the trapping field. The general technique to achieve the highest fidelity is therefore to take great care in designing the control signal (that is, the laser beam) that interacts with the ions, eliminating all undesirable effects by fine-tuning the parameters of the protocol. This constrains the design space for the control signal.

The IonQ – JQI team's idea was to sacrifice a small amount of fidelity to save a significant amount of laser power – in some cases an order of magnitude. "We consider the constraints that don't contribute significantly to the error processes when removed," explains fellow co-author Yunseong Nam, quantum theory lead at IonQ and adjunct assistant professor at the University of Maryland. "This way, while we sacrifice a minimal amount of fidelity, we can significantly increase the size of the design space, which can then be used to better optimize the power requirement."

Nam and his colleagues implemented their protocol on the JQI's programmable trapped-ion quantum hardware with five qubits. When they measured both the power and the fidelity of the gate operations, they found that they could create a maximally entangled state with their method without losing significant fidelity.

Generalizing the technique

Now that the team has carried out a successful proof-of-concept demonstration, its members plan to implement their two-qubit entangling gate in various quantum algorithms. This should allow them to verify

whether the newly developed protocol leads to an increase in overall efficiency. Linke adds that they are also exploring ways to generalize their method. “We are working on other schemes for generating entangling gates with different control parameters,” he says. “This will provide the optimal quantum gate mechanism for the particular noise or error characteristics of different devices.”

3 Rare Superconductor Discovered – May Be Critical For The Future Of Quantum Computing

https://thequantumhubs.com/rare-superconductor-discovered-may-be-critical-for-the-future-of-quantum-computing/

Research led by Kent and the STFC Rutherford Appleton Laboratory has resulted in the discovery of a new rare topological superconductor, LaPt3P. This discovery may be of huge importance to the future operations of quantum computers.

Superconductors are vital materials able to conduct electricity without any resistance when cooled below a certain temperature, making them highly desirable in a society needing to reduce its energy consumption.

They manifest quantum properties on the scale of everyday objects, making them highly attractive candidates for building computers that use quantum physics to store data and perform computing operations, and can vastly outperform even the best supercomputers in certain tasks. As a result, there is an increasing demand from leading tech companies like Google, IBM and Microsoft to make quantum computers on an industrial scale using superconductors.

However, the elementary units of quantum computers (qubits) are extremely sensitive and lose their quantum properties due to electromagnetic fields, heat, and collisions with air molecules. Protection from these can be achieved by making more resilient qubits using a special class of superconductors called topological superconductors which in addition to being superconductors also host protected metallic states on their boundaries or surfaces.

Topological superconductors, such as LaPt3P, newly discovered through muon spin relaxation experiments and extensive theoretical analysis, are exceptionally rare and are of tremendous value to the future industry of quantum computing.

To ensure its properties are sample and instrument independent, two different sets of samples were prepared in the University of Warwick and in ETH Zurich. Muon experiments were then performed in two different types of muon facilities: in the ISIS Pulsed Neutron and Muon Source in the STFC Rutherford Appleton Laboratory and in PSI, Switzerland.

Dr. Sudeep Kumar Ghosh, Leverhulme Early Career Fellow at Kent’s School of Physical Sciences and Principle Investigator said: ‘This discovery of the topological superconductor LaPt3P has tremendous potential in the field of quantum computing. Discovery of such a rare and desired component demonstrates the importance of muon research for the everyday world around us.’

29 Jun 2021

4 Rigetti Computing introduces world's first scalable multi-chip quantum processor

by Rigetti Computing

https://www.globenewswire.com/news-release/2021/06/29/2255028/0/en/Rigetti-Computing-introduces-world-s-first-scalable-multi-chip-quantum-processor.html

Rigetti Computing, a pioneer in full-stack quantum computing, announced today it is launching the world's first multi-chip quantum processor. The processor incorporates a proprietary modular architecture that accelerates the path to commercialization and solves key scaling challenges toward fault-tolerant quantum computers. Rigetti expects to make an 80-qubit system powered by the breakthrough multi-chip technology available on its Quantum Cloud Services platform later this year.

"We've developed a fundamentally new approach to scaling quantum computers," says Chad Rigetti, founder and CEO of Rigetti Computing. "Our proprietary innovations in chip design and manufacturing have unlocked what we believe is the fastest path to building the systems needed to run practical applications and error correction."

Scaling quantum computers comes with inherent challenges. As chips increase in size, there is a higher likelihood of failure and lower manufacturing yield, making it increasingly difficult to produce high-quality devices. Rigetti has eliminated these roadblocks by developing the technology to connect multiple identical dies into a large-scale quantum processor. This modular approach exponentially reduces manufacturing complexity and allows for accelerated, predictable scaling.

"Scalability is a central objective across the entire quantum computing industry. Rigetti is the first to demonstrate an elegant, effective solution to this major technical challenge," said Marko Lončar, a Harvard professor of electrical engineering working on quantum hardware, who is familiar with the company's work.

The company's multi-chip approach enables future systems to scale in multiplicative ways. Next-generation architectures currently in development at Rigetti include individual chips with more qubits, as well as advanced technologies to help connect more of these chips into larger processors. Rigetti manufactures all of its chips at its California-based captive quantum foundry.

"There is a race to get from the tens of qubits that devices have today, to the thousands of qubits that future systems will require to solve real-world problems," says Amir Safavi-Naeini, assistant professor of applied physics at Stanford. "Rigetti's modular approach demonstrates a very promising way of approaching these scales."

28 Jun 2021

5 How Best Can IT Departments Battle Attacks From Anonymous Quantum Computers?

by Alan Grau

https://www.designnews.com/industry/how-best-can-it-departments-battle-attacks-anonymous-quantum-computers?utm_medium=email&_hsmi=137284072&_hsenc=p2ANqtz-8VPMg4yzhEXACzIo_bgJu9ifV1fdfzmLNsojmLMCTXFYM3nrr0lJuIUvSztuEglMUn4BsKENeHqXb5EIlW8I1nZrE7rA&utm_content=137284072&utm_source=hs_email

Quantum computing is a special topic area in quantum information science. A traditional computer has

two states, on and off, while a quantum computer can also use a third state known as a superposition. This gives a quantum computer very unique capabilities, such as solving integer factorization very quickly. A traditional binary computer solves that particular mathematical problem slowly, whereas a quantum computer with an efficient algorithm can solve that same problem much more quickly. For example, in breaking RSA-2048, the time could be reduced from trillions of years to possibly just minutes.

Traditional computers measure their data in bits, but quantum computers utilize a 'quantum bit' or qubit. The main challenge for quantum computing is to keep qubits stable, which is a very important area of ongoing research and a requirement for the commercialization of quantum computers. As researchers build quantum computers with larger numbers of stable cubits, they can solve these difficult mathematical problems much more quickly.

The security of RSA encryption, one of today's main cryptographic algorithms, is based on the computational difficulty of factoring large integers into prime numbers. The security of Elliptic Curve Cryptography (ECC), the main alternative for RSA, is based on the difficulty in finding the discrete logarithm of a random elliptic curve element. These two algorithms form the foundation for most PKI implementation, which, in turn, provide the security for most data protection and secure communication solutions in use today.

ECC and RSA encryption can be performed quickly by traditional computers, but traditional computers would require many years to break these encryption schemes. For example, for RSA-2048, current computers require roughly 300 trillion years to break the encryption. Quantum computers change this.

Once quantum computers reach the point that enough stable qubits are attained, they will be able to solve the math problems underlying these algorithms and thereby break the encryption schemes in a matter of weeks, days, or even minutes. For RSA encryption, this is done using Shor's Algorithm. To maintain the security of data, new cryptographic algorithms must be implemented. Currently, industry organizations, researchers, and leading security companies are developing new cryptographic algorithms that are resistant to quantum computing in general and to Shor's Algorithm in particular.

The goal of these new algorithms is to ensure that they will be available to secure information and communications before the current cryptographic algorithms are broken. However, while quantum computers are massively faster at solving many mathematical problems, they are not simply universally faster at all processing tasks and offer an advantage only for a limited set of mathematical problems. By using different mathematical approaches, it is possible to develop cryptographic algorithms that can be efficiently executed on traditional computers but that are resistant to attacks from quantum computers.

Basically, the solution is a combination of new math alongside new PKI tools. Thankfully, some of the best minds on the topic have already been researching the most optimal quantum-resistant algorithms from a security and performance standpoint.

What is the quantum apocalypse?

The inevitable day when quantum computing renders RSA and ECC encryption algorithms obsolete could be so crippling to society that the security sector has deemed it the "Quantum Cryptographic Apocalypse." The hype isn't unfounded. RSA and ECC encryption are used to secure every data source and system across industries: factories, data farms, utilities, e-commerce and banking systems, transportation, communication networks, and much more.

When enough stable qubits are attained in a quantum computer, the current cryptographic algorithms will be rendered insecure. That point in time is known as the 'quantum apocalypse.' While it will take time to get there, experts estimate that the date is only 6-10 years away.

There has been a great deal of research to find the next generation of quantum-resistant algorithms, as well as standards development on PKI certificates, that can act as an operational bridge between the current generation of algorithms and post-quantum resistant algorithms. In July 2020, the National Institute of Standards and Technology (NIST) announced the third-round candidates consisting of 7 finalists and eight alternate algorithms.

While quantum computing is still in the development phase, the Quantum Apocalypse is coming.

Sound scary? Well, it can be. If you have information, systems, and devices that need to be kept secure and private for years and decades to come, your organization needs to prepare now.

Yes, quantum computers are complex and expensive systems that, at first, will only be affordable for major international technology organizations. However, their use can then spread to various nation-states and eventually to cybercriminals and hackers.

The good news is that there are steps that the manufacturing and tech industries can take now.

Phased Migration to Quantum-Safe Cryptography

Migrating to quantum-safe crypto algorithms will require planning and updates to multiple systems. All need to be protected. A company's internal data management and communications systems, as well as third-party applications, servers, and systems, will all need to be updated.

Engineers and development teams must begin planning now to migrate to quantum-safe crypto. For factories and large enterprises, these measures will be a major undertaking.

The following six steps are required for either direct or hybrid migration plans.

(i) Upgrade to a quantum-safe PKI security infrastructure

The first step towards migrating to quantum-safe cryptography is to upgrade the PKI infrastructure, including the certificate authority, with support for quantum-safe crypto algorithms. Rather than trying to upgrade internal PKI systems, this may be an ideal time for companies to migrate to a commercial Certificate Authority (CA), such as Sectigo, which can provide commercial support for quantum-safe crypto algorithms.

Whether moving to an in-house PKI system or adapting a solution from a commercial vendor, it is critical that the CA provide support for quantum-safe crypto algorithms and quantum-safe certificate issuance. If the IT security team chooses to use hybrid certificates, they must select a CA that supports both hybrid certificates and pure quantum-safe certificates.

Hybrid certificates contain both a traditional ECC or RSA key and signature and a new quantum-safe key and signature. This allows systems that have been upgraded to support quantum-safe algorithms to use the newer algorithms, while older systems can still use the certificate by utilizing the traditional algorithm. This can also allow interoperability of older and newer systems during the migration period.

Once an organization upgrades its existing CA or selects a new CA, the CA must issue a new quantum-safe root and intermediate certificate.

(ii) Update server applications to recognize and use new crypto algorithms.

Migrating to quantum-safe crypto requires updating the crypto libraries used by server applications to support both the new crypto algorithms and the new quantum-safe certificate formats, including hybrid certificates if used. If hybrid certificates are used, server applications will need to recognize

and process both traditional RSA/ECC certs and hybrid certs containing quantum-safe crypto keys. This requires the server applications to distinguish between the two different certificate types and handle each with the proper crypto algorithm for that certificate type.

(iii) **Update the client crypto algorithms.**

IT and development teams will also need to update a wide range of client applications to use quantum-safe crypto algorithms. Once fully and safely upgraded, administrators can discontinue the use of traditional RSA/ECC keys/certificates in client applications and instead use the new quantum-safe equivalents.

The exception to this policy is a client application that communicates with multiple server applications that may not all be simultaneously upgraded to quantum-safe crypto. In this case, hybrid certificates will allow the client to work with servers supporting traditional RSA/ECC crypto while at the same time, use quantum-safe algorithms with servers that support these newer algorithms.

(iv) **Install quantum-safe roots on all systems.**

Each security system utilizing PKI has a trusted root store. This root store contains the certificates for the root and intermediate CAs that issue certificates within the PKI system. Once systems have been updated to support quantum-safe crypto algorithms, these root stores must also be updated to add the new root and intermediate certificates.

(v) **All connected devices/applications will need quantum-safe certificates.**

After IT teams have updated all a company's systems to support quantum-safe crypto, they must issue new certificates and install them on all the endpoints. Once completed, each device can begin using quantum-safe crypto algorithms, as enabled by the new certificates.

(vi) **The Final Step – Get rid of the old.**

The final step in migrating to quantum-safe crypto is to deprecate the traditional encryption algorithms, so they are no longer used. This can be done gradually on applications and systems as they are migrated to the new algorithms. After all, systems have been migrated, the root ECC and RSA certificates should be revoked, ensuring they are not used by any systems.

Summary

Quantum computers capable of breaking traditional crypto algorithms will arrive within the next decade. Yes, at first, they will be limited to big international companies and nation-states, but eventually, quantum computing will be affordable for the average cybercriminal and hacker.

For most organizations, the task of migrating to new, quantum-safe crypto algorithms will require a major, well-planned effort spanning a variety of internal development teams and third-party vendors. Companies will have to upgrade the PKI systems that they are using along with the company-wide applications using these certificates.

Hybrid certificates enable a safe, gradual migration of systems, but ultimately all systems using ECC or RSA encryption must migrate to new, quantum safe-crypto algorithms. Otherwise, an organization's applications and systems will be vulnerable to attacks using quantum computers.

25 Jun 2021

6 UCL researchers Find Use for Abstract Task Implemented in Google's 'Quantum Supremacy' Experiment

by Matt Swayne

https://thequantumdaily.com/2021/06/25/ucl-researchers-find-use-for-abstract-task-implemented-in-googles-quantum-supremacy-experiment/

UCL research shows that pseudorandom circuits, recently implemented in Google's 'quantum supremacy' experiment, can be used to simulate properties of quantum systems that are hard to compute classically. UCL researchers also think that this randomness might help reduce the impact of errors in the operation of quantum computers.

In October 2019, Google said its research lab in Santa Barbara had achieved 'quantum supremacy' using their quantum processor named 'Sycamore' – a two-dimensional array of 54 qubits.

Google's researchers used their superconducting quantum processor to perform a random sampling task that they asserted demonstrates the experimental realisation of quantum supremacy because by Google's estimate (in 2019) an equivalent task by a state-of-the-art classical supercomputer would take approximately 10,000 years.

This random sampling task consisted of sampling from the output of pseudorandom circuits, that is Google's researchers applied a sequence of one- and two-qubit gates, drawn at random from some available set of gates, and measured the outcome. This task is arguably rather abstract, and at the time of Google's announcement other researchers debated that while the result was commendable, it wasn't a true demonstration of quantum supremacy as the random sampling task used had no known useful physical application.

UCL researchers Dr Jonas Richter and Dr Arijeet Pal argue in Physical Review Letters that pseudorandom circuits, as realized in Google's seminal experiment, are not just abstract tools, but can form tailor-made building blocks to simulate certain aspects of quantum many-body systems on noisy intermediate scale quantum (NISQ) computers. Their research opens a route to formulate algorithms using pseudorandom circuits that better tackle physical problems.

Co-author Dr Jonas Richter (UCL Physics & Astronomy and UCLQ) said: "Many-body system simulations are notoriously challenging and sometimes intractable even with modern supercomputers, however they would be natural for a quantum device. By adapting Google's random sampling task, we have designed an efficient algorithm that can run on near-term quantum hardware. We show that researchers can use this algorithm to explore difficult to simulate aspects of quantum many-body systems. Furthermore, we believe researchers could use this tool to explore systems that are difficult to find or don't exist in nature, which may lead to fundamental discoveries."

In the study, the researchers detail an efficient algorithm to simulate hydrodynamics. Hydrodynamics describes the flow of spin or particle densities in quantum systems. Their work also suggests that meaningful simulations of quantum hydrodynamics should be possible with realistic error rates on near-term quantum devices.

Co-author Dr Arijeet Pal (UCL Physics & Astronomy and UCLQ) said: "We show that randomness can be useful – that the abstract sampling task implemented by Google's research team can be of practical use on the noisy quantum computers we have today, and that randomness may in fact be the key to mitigate the naturally occurring errors of quantum computers."

Richter and Pal plan to test their algorithm on current quantum hardware and investigate whether the intrinsic randomness of the quantum state might actually mitigate the harm caused by the inevitable errors quantum computers face in their normal operation.

A quantum computer harnesses laws of physics that are normally seen only at the atomic and subatomic level (for instance, that particles can be in two places simultaneously). Quantum computers could be more powerful than today's super computers and capable of performing complex calculations that are otherwise practically impossible.

However, currently available quantum computers have relatively few quantum bits and are subject to interference. These noisy intermediate scale quantum computers are prone to errors and do not yet have the computational resources needed to directly simulate large quantum systems.

While the applications of quantum computing differ from traditional computers, they will enable us to solve certain types of problems that cannot be solved on classical computers. These include problems that involve quantum mechanics directly such a drug development, but will also help optimise the solutions to complex everyday problems such as transport and logistics.

This research was funded by the European Research Council under the European Union's Horizon 2020 research and innovation programme.

24 Jun 2021

7 MIT Makes a Significant Advance Toward the Full Realization of Quantum Computation

by michaela jarvis

https://scitechdaily.com/mit-makes-a-significant-advance-toward-the-full-realization-of-quantum-computation/?utm_medium=email&_hsmi=137284072&_hsenc=p2ANqtz-9hzfH-xf65ciLTgtqMsTRIpMABpM2Y1JRtTnfjvx-4gr4UpjYD-I0k1wuQPOD3TUtclDm58fC77xTBBXu11643HpjDbQ&utm_content=137284072&utm_source=hs_email

MIT researchers have made a significant advance on the road toward the full realization of quantum computation, demonstrating a technique that eliminates common errors in the most essential operation of quantum algorithms, the two-qubit operation or "gate."

"Despite tremendous progress toward being able to perform computations with low error rates with superconducting quantum bits (qubits), errors in two-qubit gates, one of the building blocks of quantum computation, persist," says Youngkyu Sung, an MIT graduate student in electrical engineering and computer science who is the lead author of a paper on this topic published on June 16, 2021, in Physical Review X. "We have demonstrated a way to sharply reduce those errors."

In quantum computers, the processing of information is an extremely delicate process performed by the fragile qubits, which are highly susceptible to decoherence, the loss of their quantum mechanical behavior. In previous research conducted by Sung and the research group he works with, MIT Engineering Quantum Systems, tunable couplers were proposed, allowing researchers to turn two-qubit interactions on and off to control their operations while preserving the fragile qubits. The tunable coupler idea represented a significant advance and was cited, for example, by Google as being key to their recent demonstration of the advantage that quantum computing holds over classical computing.

Still, addressing error mechanisms is like peeling an onion: Peeling one layer reveals the next. In this

case, even when using tunable couplers, the two-qubit gates were still prone to errors that resulted from residual unwanted interactions between the two qubits and between the qubits and the coupler. Such unwanted interactions were generally ignored prior to tunable couplers, as they did not stand out – but now they do. And, because such residual errors increase with the number of qubits and gates, they stand in the way of building larger-scale quantum processors. The Physical Review X paper provides a new approach to reduce such errors.

"We have now taken the tunable coupler concept further and demonstrated near 99.9 percent fidelity for the two major types of two-qubit gates, known as Controlled-Z gates and iSWAP gates," says William D. Oliver, an associate professor of electrical engineering and computer science, MIT Lincoln Laboratory fellow, director of the Center for Quantum Engineering, and associate director of the Research Laboratory of Electronics, home of the Engineering Quantum Systems group. "Higher-fidelity gates increase the number of operations one can perform, and more operations translates to implementing more sophisticated algorithms at larger scales."

To eliminate the error-provoking qubit-qubit interactions, the researchers harnessed higher energy levels of the coupler to cancel out the problematic interactions. In previous work, such energy levels of the coupler were ignored, although they induced non-negligible two-qubit interactions.

"Better control and design of the coupler is a key to tailoring the qubit-qubit interaction as we desire. This can be realized by engineering the multilevel dynamics that exist," Sung says.

The next generation of quantum computers will be error-corrected, meaning that additional qubits will be added to improve the robustness of quantum computation.

"Qubit errors can be actively addressed by adding redundancy," says Oliver, pointing out, however, that such a process only works if the gates are sufficiently good – above a certain fidelity threshold that depends on the error correction protocol. "The most lenient thresholds today are around 99 percent. However, in practice, one seeks gate fidelities that are much higher than this threshold to live with reasonable levels of hardware redundancy."

The devices used in the research, made at MIT's Lincoln Laboratory, were fundamental to achieving the demonstrated gains in fidelity in the two-qubit operations, Oliver says.

"Fabricating high-coherence devices is step one to implementing high-fidelity control," he says.

Sung says "high rates of error in two-qubit gates significantly limit the capability of quantum hardware to run quantum applications that are typically hard to solve with classical computers, such as quantum chemistry simulation and solving optimization problems."

Up to this point, only small molecules have been simulated on quantum computers, simulations that can easily be performed on classical computers.

"In this sense, our new approach to reduce the two-qubit gate errors is timely in the field of quantum computation and helps address one of the most critical quantum hardware issues today," he says.

8 Redefining Quantum Computations Using Classical Computers

by ritika sagar

https://analyticsindiamag.com/redefining-quantum-computations-using-classical-computers/

"The most important application of quantum computing in the future is likely to be a computer simulation of quantum systems because that's an application where we know for sure that quantum systems, in general, cannot be efficiently simulated on a classical computer" – British physicist David Deutsch.

Going by David's statement, the Institute for Quantum Computing (IQC), in collaboration with the University of Innsbruck, has proposed solving complex computing problems using measurement-based algorithms within a feedback loop with a regular computer.

This novel computing method serves as a key tool in bringing academics to the forefront of developments in quantum computing, allowing new algorithms and experiments to take researchers much closer to commercial applications and discoveries of the technology.

Christine Muschik, Principal Investigator at the Institute for Quantum Computing (IQC), believes that quantum computers of the future can be used in applications such as removing carbon dioxide from the atmosphere, developing artificial limbs, and designing more efficient pharmaceuticals.

No need for quantum gate-based computer

The study by Muschik's team is focused on quantum calculations that do not require quantum gate-based computers. The team designed an algorithm to carry out a hybrid quantum-classical computation by combining a sequence of measurements on an entangled quantum state with a quantum-classical computation.

To use the principles of measurement-based quantum computation, they developed a new approach to Variational Quantum Eigensolver (VQE).

Ideally, existing VQE protocols based on circuit models use gates that are applied on an initial state. To obtain an output state, as close as possible to the target state, the variational parameters must be optimised. The new approach to VQE protocols is based on a measurement-based model of quantum computation (MBQC).

MBQC can prepare an entangled state and then perform single-qubit measurements to realise the computation. Quantum computing is made possible through both circuit-based and measurement-based models. While both are similar in terms of resource scaling, there is one difference. The circuit-based model's capabilities are constrained by the number of available qubits and gates that can be executed. In comparison, the needed coherence times and error thresholds are somewhat relaxed for MBQ. The new variational technique based on MBQC is called the measurement-based VQE (MBVQE).

The researchers' new protocols determined the ground state of a target Hamiltonian, a prototypical task for VQEs with wide-ranging applications. The fundamental concept for this was to employ a customised entangled state, called a 'custom state'. It enabled exploration of a particular corner of the system's Hilbert space. This custom state contains auxiliary qubits that, when measured, change the output qubits' states. A traditional optimisation approach is used to control the measurement bases and the resulting variational changes in the state. This approach is conceptually and practically distinct from normal VQE schemes.

After introducing the MB-VQE framework, researchers designed two measurement-based VQE techniques. Firstly, they demonstrate a method for constructing variational state families using the toric code model with local perturbations. Second, they demonstrated a direct conversion of circuit VQEs to MB-VQEs.

The variational state family is the same for the circuit and measurement-based techniques, but the implementations are distinct because the MBVQE requires more resources and is modified only via single-

qubit measurements. While MB-VQE is platform-independent, it enables complicated quantum calculations in systems with lengthy gate sequences, or the realisation of entangling gates is difficult.

This theoretical research offers a new way of thinking about optimisation algorithms. MB-VQE in particular expands the toolset of variational computing by providing additional paths for experiments with photonic quantum systems. Researchers no longer have to deal with fussy and sensitive resources, allowing them to construct feedback loops specific to the datasets their computers are researching.

23 Jun 2021

9 Quantum computing may transform cybersecurity eventually – but not yet

by Derek B. Johnson

https://www.scmagazine.com/home/security-news/encryption-data-security/quantum-computing-may-transform-cybersecurity-eventually-but-not-yet/

The hype cycles that come with emerging technologies can be perilous waters for early adopters and buyers.

From the immutable yet seemingly impractical blockchain to artificial intelligence systems that are really just machine learning systems (which in turn are often really just rules-based software with data analytics), it's common for marketing departments to blur the lines between innovation and grift when selling new technologies, and for businesses to get snookered.

One field that does appear to have long-term transformative potential is quantum computing and its cybersecurity cousin, quantum code breaking. But before we get started: actual quantum computers are not here. Not yet.

A small group of government-funded labs, industry titans and startups are toiling away, steadily increasing the number of qubits their supercomputers are capable of processing each year, but it will likely be a long time before businesses and other organizations can realistically buy one, or unleash its exponential computing power on their organization's problems.

However, a related issue is likely to be closer on the horizon: protecting the computers, systems and data we have today from the quantum code breaking techniques of tomorrow. While experts don't know when or where a quantum computer will emerge that can break most forms of classical encryption, most agree that enterprises will need to replace their encryption protocols well in advance of that day. Beyond that, the threat of foreign governments or other actors harvesting your encrypted data today to crack it with quantum computers tomorrow is a real concern.

While government agencies and standards bodies are currently racing to test and vet new quantum resistant algorithms for widespread consumption, a small but growing industry of vendors has already popped up offering to sell such protections to the broader public. That leaves many in the business world facing thorny questions like when they should buy or implement such solutions, when is it too soon and when is it too late?

"If you are not paying attention, you will get left behind," said Dan Meacham, chief information security officer at Legendary Entertainment when asked for his thoughts on moving to quantum resistant encryption.

Still, like many in business today, Meacham finds himself struggling to separate the substance from the marketing.

"Innovation is a good thing ... I think there is a lot of 'quantum' that really isn't quantum – much like how AI and machine learning really are not AI or machine learning in some solutions," he said. "At best, we need to partner with the vendor to fully understand what are we trying to solve, and if a quantum solution really is the answer."

Setting the stage

The estimated size of the quantum encryption market is tiny, reflecting both the nascent state of the technology and likely a lack of awareness or urgency on the part of buyers. Forecasters peg the global market today at between $100 - $200 million, but predict robust compound growth over the next five years. The overall encryption market is exponentially larger than that, and is likely to grow substantially over the next decade as more organizations switch out their classical encryption with quantum resistant versions.

Unlike other emerging technologies such as blockchain – where it's far from clear the practical applications and use cases will ever justify the hype and speculation it unleashed – most experts in quantum physics and cybersecurity do think quantum-based encryption will become essential to data security in the not-too-distant future.

It's that last part, figuring out just how distant the future is, that makes purchasing in this area today so tricky.

Quantum supercomputers managed by the federal government and industry titans like IBM and Google have been quietly chugging along for years, processing ever higher numbers of qubits. While each new development been met with excitement and reinforced the technology's potential, most experts believe we are still between 5-10 years away from processing the number of qubits capable of breaking classical encryption algorithms like RSA.

"It's not just the number of qubits, it's also the error rates and the accuracy that one needs to get" to break modern forms of encryption like RSA, said Josyula Rao, chief technology officer for IBM during an event hosted by national security think tank Center for Strategic and International Studies in June.

Rao said IBM's research on quantum supercomputers indicates that the number of qubits required to bust today's encryption would require processing approximately 6,200 qubits and 2.7 billion operations. IBM said last year that they are working to build a quantum computer capable of processing 1,000 qubits by 2023.

"So we do have some ways to go before we get to the error rates we need to field a machine and run programs that can actually pose a threat to the security and cryptography that we've deployed today," he said.

Others in industry dissent from that view, or argue that the concept of "technological surprise" tells us there's at least some chance that experts are underestimating the maturing pace of the technology. Lisa O'Connor, managing director of global security research and development at Accenture said "we may be closer than we think" to the kind of breakthroughs that would move quantum-based code breaking from the theoretical to the real.

"It doesn't take solving all, it takes targeted focus and it takes targeted focus at an adversary going after that communication or that thing they want, past or present," O'Connor said.

Post-Quantum, a British company founded in 2009, sells encryption and identity software solutions based on the Classic McEliece algorithm (currently a National Institute for Standards and Technology finalist). In an interview, CEO Andersen Cheng said that he while the timeframe for a commercially available quantum computer may be a decade or more away, he believes military and intelligence agencies that employ teams of hackers are probably closer to developing something that can break classical encryption. If such a breakthrough were to happen as part of a classified government project, he worries the country behind it would have numerous incentives to keep it secret and use it to conduct digital espionage and intelligence gathering.

"I'm not talking about a [quantum computer] that JP Morgan can buy to do their own trading analysis or credit risk analysis, I'm talking about the sheer power to do code breaking," Cheng said. "I can almost bet my house that whoever's got a functional computer [first] will be keeping quiet about it, They will not be going to the press. They will not be like Google, claiming quantum supremacy."

A quantum of (buying) solace on the horizon

NIST has spent years carefully vetting different types of algorithms that could be capable of withstanding quantum codebreaking in the future. The structure of NIST's program reflects our current imperfect understanding, as well as the possibility that things could go wrong. There are currently 15 separate finalist algorithms being evaluated by the agency, after cutting dozens of other potential candidates in a multi-round process.

The agency plans to pick a handful of diverse algorithms to standardize by the end of this year, with the rulemaking and public comment process expected to push finalized encryption standards to 2024 or 2025. This could provide much needed clarity to potential buyers about the technologies and processes that will make their way into procurement, contracting and industry standards.

However, NIST officials have given clear, unambiguous advice to businesses in past years when it comes to buying such solutions today: don't. At least not until they finish the new standards.

"We still recommend waiting to purchase commercial products for quantum resistance," Dustin Moody, a NIST mathematician who leads the post-quantum cryptography project, told SC Media in an email this month.

Moody was blunt about NIST's view of the potential dangers that come with buying quantum resistant encryption products today, noting that even as the process has increasingly tested each finalist, "we have seen algorithms broken in each round of the process."

Due to the time and financial costs that come with switching out encryption protocols, as well as the likelihood that NIST's chosen algorithms will underpin future federal contracting or industry standards, he stressed that "it's important to get it right the first time."

"By purchasing and implementing early, you risk using algorithms that are not the ones that end up being standardized. You risk not being interoperable with those that will use the standard," Moody said. "Although there is always a security risk that a cryptographic algorithm may be broken [or] attacked, the risk is higher using algorithms that have not been standardized – particularly in this field of post-quantum cryptography."

NIST does not discount the possibility of data harvesting. In fact, those concerns helped drive the creation of the project in the first place. However, Moody noted that this threat, while real, is likely less dire than perceived.

It's true that large-scale quantum computers will eventually be able to completely break encryption that relies on asymmetric, public-key algorithms, but much of our data is encrypted using symmetric key block ciphers, and here the impact is likely more modest. Cryptographers believe that using larger key sizes for their symmetric encryption would be sufficient to protect such data from quantum codebreaking, though even here there is uncertainty since many symmetric key algorithms rely on asymmetric encryption protocols to establish a shared key.

However, most encryption experts believe that switching over to these new encryption protocols will be a laborious process, taking up to 1-2 years for most organizations and as long as five years for larger enterprises. In the meantime, NIST standards do allow for the use of hybrid solutions that use both classical encryption and newer quantum-resistant algorithms, as long as the classical algorithm is FIPS compliant, though the agency warns that these standards "were not necessarily designed to provide post-quantum security."

Meanwhile, the National Security Agency's cybersecurity division has said it expects to incorporate one of the lattice-based algorithm signature and key encapsulation method to guard their national security systems, and a hash-based signature for certain "niche" applications. Even here, the agency provides notable caveats as to their long-term reliability.

"At the present time, [we] do not anticipate the need to approve other post-quantum cryptographic technologies for NSS usage, but recognize circumstances could change going forward," the agency said. "A variety of factors – including confidence in security and performance, interoperability, systems engineering, budgeting, procurement, and other requirements – could affect such decisions."

Denis Manich, chief technology officer at Qrypt, told SC Media that his company is mainly interested in selling to certain industries with extremely sensitive data and high regulatory requirements around keeping them safe. He pointed to a partnership Qrypt did with Telefonica earlier this year to incorporate their random number generating technology into the Spanish telecom's cloud-based virtual data centers.

"Our primary goal is to leverage banking, telecoms and large industries that have a compliance mandate and critical infrastructure," Manich said when asked about the kind of customers Qrypt pursues.

Cheng said the sectors with the most urgent timelines for implementing quantum-resistant encryption are likely government agencies or enterprises which have data that they have to keep for the next ten, twenty or thirty years, like health care organizations.

Information asymmetry

The underlying math and physics behind quantum computing can be unbearably complex, even for many IT and cybersecurity practitioners with highly technical backgrounds in other fields.

At the same time the need for data encryption that can withstand post-quantum hacking is nearly universal, as relevant to the small, mom and pop business as it is to Fortune 500 companies and government agencies. This has created an information asymmetry problem between consumers and sellers, with many businesses lacking the in-house expertise to spot lemons or snake oil solutions.

Multiple encryption vendors reached by SC Media cited two features they claim are key to responsibly selling quantum cryptographic solutions today.

Several have tied their products to algorithms that are finalists in the NIST process, something they say greatly increases the odds that they will be relevant to a post-quantum environment after three rounds of vetting.

"What I want to say is we are working closely with NIST and we understand the position when they give such warnings," said Dr. Ali El Kaafarani, CEO and founder of PQShield and a visiting professor at Oxford University's Mathematical Institute.

Kaafarani and others acknowledged that the potential for lemons or snake oil in the post-quantum cryptography market is high. He gave three examples of what he considers red flags for potential buyers: vendors that are not using one of the finalist NIST algorithms under consideration; those who sell anything resembling "crypto box" devices, rather than a process or solution for building encryption into your existing IT infrastructure; and solutions that are only designed to support a single algorithm.

Kaafarani, Cheng and others also strongly endorsed the concept of crypto agility – essentially designing your encryption protocols in a way that can facilitate the swift replacement of the underlying algorithm. The logic here is that future research may discover new attacks or weaknesses that can be exploited to render any one particular algorithm obsolete. It's why NIST will ultimately choose multiple algorithms to standardize and hold another handful close at hand as backup options.

"Regardless of when NIST finalizes any quantum-resistant encryption, or when [they] become capable of breaking today's encryption, crypto-agility is a capability that is needed today," said JupiterOne CISO Sounil Yu.

One startup, Qrypt, has intentionally foregone using any of the quantum resistant algorithms being considered, instead relying on a much older form of classical encryption called one-time pad encryption, to generate random numbers for encryption keys. Though it was first developed back in the 1940s, cryptographers and mathematicians believe this form of encryption is unbreakable and capable withstanding brute force attacks from a quantum computer, provided the parties never use the same key twice. It's the method that was used by the White House to protect communications for their direct line to Moscow during the Cold War.

We have already seen commercial technologies based on one of the most popular methods of quantum encryption fail. In 2010, researchers from the University of Toronto in Canada released research demonstrating how they were able to break the quantum cryptographic protocols used by encryption startup ID Quantique, namely by exploiting errors in the process they used to generate random numbers and create secret keys. While this error was correctable, it's a reminder of how difficult it can be to give security assurances around a still developing technology.

More recently, NIST has had to reevaluate one of their finalist algorithms, dubbed Rainbow, after researchers discovered two new attacks that substantially reduce the number of security bits and weaken its encryption.

Cheng, who has worked in the quantum encryption space for more than a decade, said the number of companies popping up with little backgrounds in the field, using unvetted algorithms or making outsized promises around the potential risks. Executives should proceed with caution, he warned, lest they unwittingly create new security problems in the future.

"This is the industry we are seeing today, which is getting dangerous by the way, because ... if you do it purely from an academic angle, it will cause what we call secondary characteristics [that classic forms of encryption like] RSA or elliptic curve never had," he said.

10 The paradox of post-quantum crypto preparedness

by Graham Steel

https://www.helpnetsecurity.com/2021/06/23/post-quantum-crypto-preparedness/

Preparing for post-quantum cryptography (PQC) is a paradox: on the one hand, we don't know for sure when, or perhaps even if, a large quantum computer will become available that can break all current public-key cryptography. On the other hand, the consequences would be terrible – hijacked code updates, massive sensitive data exposure – and the migration process so complicated that we have no choice but to start preparing now. But what can we do, without wasting resources, to be ready and to reassure our customers that we're ready?

Fortunately, there is a way to prepare for PQC that not only mitigates risk, but also gives us a number of immediate security and resilience benefits. Two recent reports, one from NIST and another from ENISA hold the key. In this article, we'll show how you can use the takeaways from these reports to build a PQC plan for your organization with an instant return on investment, even if a large quantum computer turns out to be decades away.

The right kind of inventory

The NIST report, **Getting Ready For Post Quantum Cryptography**, covers the development of an inventory and a migration playbook. It is common sense to start your post-quantum planning with an inventory of the cryptography you use, but as the report makes clear, just listing the algorithms each application employs is a waste of time. For the inventory to have value, it must detail how the cryptography is used, and for what. NIST recommends that you identify automated tools to assist with this task, since retrieving this level of detail by hand would be far too time-consuming.

The reason the inventory needs this rich information becomes clear when you come to build the migration playbook. PQC won't be a simple drop-in replacement for existing cryptography. There will most likely be a number of candidate algorithms with different trade-offs in terms of execution time, key size, output size, and other characteristics.

For each current use of public-key cryptography, you will have to choose the best replacement that suits the constraints of that usage. NIST gives a 15-point bulleted list of considerations on the usage that you will need to take into account. This includes technical considerations like performance, but also business considerations, like product lifetime and compliance requirements.

The value of NIST's 15-point list is that it can guide the cryptography inventory work. By making sure the inventory contains enough information to respond to these 15 questions, we can make sure that we're preparing in the most efficient way possible to build the migration playbook when the time comes.

The good news about this kind of rich cryptography inventory is that it has immediate business benefits, long before the arrival of a large quantum computer, as part of good cryptography management practice. First, it will allow you to eliminate weak or non-compliant cryptography that may be in use. Mistakes with cryptography are one of the most common application security flaws, and errors such as hard-coded keys or weak block cipher modes are easily exploited. Second, it can be used to demonstrate compliance to auditors, who are becoming increasingly studious of the use of cryptographic controls. Finally, it has benefits for resilience: an inventory that includes cryptographic keys and certificates allows for rapid response to

compromises. For these business benefits to be realized, the inventory needs to be always up to date – another reason why automation is key.

Mitigating today's quantum risk

Setting up the inventory and the migration playbook is all we need if we have time to wait for the NIST standardization process to conclude. But what if we need PQC now? This might be the case if we have data that needs to be kept confidential for the long-term, or if we're shipping an embedded product now that needs to be able to verify code updates in the next 20 years. Or we might just need to reassure our customers that our critical applications will continue to function securely if a large quantum computer becomes available sooner than we were expecting.

The ENISA report Post Quantum Cryptography: Current State and Quantum Mitigation gives a roadmap for this situation. There are essentially two options if you need to mitigate quantum risk now: use a hybrid post-quantum and pre-quantum scheme, or use pre-shared keys.

Under a hybrid scheme, you'll need to select one of the most promising candidates from the NIST standardization process and use it in combination with a classical scheme like RSA. You need to combine them in such a way that security of one of the algorithms is enough to guarantee security of the result, whether that result is a signature on a document, or a key to be used for encrypting data. Researchers have been experimenting with these ideas for some time, but the ENISA report gives a succinct description of how to do this.

In practice, it is likely that PQC will be phased-in this way even after the standardization process concludes, while confidence builds in the security of the selected candidates, so knowledge gained from these experiments will be invaluable. Open-source implementations of all the remaining candidates in the process are already available.

Using pre-shared keys involves injecting extra key material into an exchange that will keep the final result secure even if the public-key scheme is later broken. This is only feasible if you can maintain state for these exchanges. Again, this is a practice that has been known about in the research world for some time, but the ENISA report explains how you can experiment with it yourself.

Equipped with the right kind of cryptographic inventory, a migration playbook, and knowledge gained from hybrid-scheme experiments, we can take a rational approach to the post-quantum paradox, with no need to panic or play down the threat. Adopting good cryptography management practices now gives us immediate benefits – and peace of mind for us and our customers for the post-quantum future.

22 Jun 2021

11 NIST Publishes Ransomware Guidance

by Sarah Coble

https://www.infosecurity-magazine.com/news/nist-publishes-ransomware-guidance/

The National Institute of Standards and Technology (NIST) has published new draft guidance for organizations concerning ransomware attacks.

The Cybersecurity Framework Profile for Ransomware Risk Management features advice on how to defend against the malware, what to do in the event of an attack, and how to recover from it.

NIST's Ransomware Profile can be used by organizations that have already adopted the NIST Cybersecurity Framework and wish to improve their risk postures. It can also help any organization seeking to implement a risk management framework that deals with ransomware threats.

Included in the Ransomware Profile are steps that can be followed to identify and prioritize opportunities for improving their ransomware resistance. Users will learn how to prevent ransomware attacks and how to manage ransomware risk effectively.

Basic measures mentioned in the guidance include keeping computers fully patched, using antivirus software, blocking access to known ransomware sites, and only permitting authorized apps to be used.

Organizations are also advised to ensure scans are automatically conducted on emails and flash drives, to restrict the use of personally owned devices, to limit the use of accounts with administrative privileges, and to avoid the use of personal apps.

Another defensive tactic against ransomware that the guidance advocates is conducting security awareness training to educate employees about the dangers of opening files sent from unknown sources or clicking on links.

NIST says planning ahead will help organizations that do succumb to ransomware to recover faster. It advises creating an incident recovery plan, implementing a comprehensive backup and restoration strategy, and maintaining an up-to-date list of internal and external ransomware attack contacts.

NIST intends for the new draft guidance to be used in conjunction with the NIST Cybersecurity Framework, other NIST guidance, and guidance issued by the Department of Homeland Security and the Federal Bureau of Investigation.

Those who wish to comment on the new draft Ransomware Profile have until July 9 to send their feedback to the Institute. A revised copy will then be released and a second commentary period held before a final document is published.

12 Optimal two-qubit circuits for universal fault-tolerant quantum computation

https://www.nature.com/articles/s41534-021-00424-z

Authors study two-qubit circuits over the Clifford+CS gate set, which consists of the Clifford gates together with the controlled-phase gate $CS = diag(1, 1, 1, i)$. The Clifford+CS gate set is universal for quantum computation and its elements can be implemented fault-tolerantly in most error-correcting schemes through magic state distillation. Since non-Clifford gates are typically more expensive to perform in a fault-tolerant manner, it is often desirable to construct circuits that use few CS gates. In the present paper, authors introduce an efficient and optimal synthesis algorithm for two-qubit Clifford+CS operators. Their algorithm inputs a Clifford+CS operator U and outputs a Clifford+CS circuit for U, which uses the least possible number of CS gates. Because the algorithm is deterministic, the circuit it associates to a Clifford+CS operator can be viewed as a normal form for that operator. We give an explicit description of these normal forms and use this description to derive a worst-case lower bound of $5\log_2(\frac{1}{\epsilon}) + O(1)$ on the number of CS gates required to ϵ-approximate elements of SU(4). Their work leverages a wide variety of mathematical

tools that may find further applications in the study of fault-tolerant quantum circuits.

21 Jun 2021

13 For long, strong passwords

by Surit Doss

https://www.telegraphindia.com/science-tech/passwords-are-your-biggest-online-security-threat/cid/1819497

The biggest threat to your online security is your passwords. Many of us face a problem memorising them, thinking up unique ones, and remembering them for each site we visit.

Eventually, we end up using the same one across multiple sites. This is risky as a hacker needs to breach one password to gain access to all your data. And changing your password is tiresome. How do we overcome this?

Password manager

Chrome comes with a password manager. It is now improving its password manager in four upgrades. Users can import passwords from other password managers and bring them within the security fold of Google. There is deeper integration between Chrome and Android, and passwords can be used across both websites and apps.

A key addition is that Chrome will identify and fix weak passwords. Note that a simple password such as Ravi123# is not necessarily a weak one. It can be a strong password but becomes weak if used across multiple sites.

A longer and stronger password can challenge a hacker into trying to breach it. And when he breaches one, he can get into other accounts. Also, passwords with variations can be at risk. You may adopt a password pattern, make a few variations and use it for different websites. This, too, is risky.

As soon as it detects a breach, Chrome will warn users and help fix the problem with a single tap.

AI technology at work

Working under the hood is the AI technology called Duplex. Duplex uses natural conversation to get things done. This technology helps you perform tasks on the web like buying tickets, ordering food and checking in for flights. AI also helps your Google Assistant in browsing, scrolling, clicking and automatically filling up forms. This technology will now help you create a strong password for sites and apps when Chrome concludes that your credentials have been compromised.

Syncing your data

This feature of automated password changes is rolling out gradually in Chrome to users who sync their passwords. Turning on sync means you will see the same information on all your devices. These include bookmarks, history and open tabs, passwords, payment information and addresses, phone numbers and more.

You can choose what information you want synced. Open Chrome. On the top right-hand corner, click on the three dots and go to Settings. Under "You and Google", click on "Sync and Google Services". To find out what you are syncing, select "Review your synced data". This will open a webpage to show what is being synced.

Go back to "Sync and Google services" in Settings. Under "You and Google" click on "Manage what you sync". I choose to sync everything but you can turn off anything that you do not want to be synced to your account.

Until you get the update for automatic password changes, you can manually control the entire experience and change your password. This can be a big help if a site is not supported by the change. Chrome's password manager can always help you create strong and unique passwords for your many accounts.

Google's machine-generated passwords

Sync has to be turned on for Chrome. Go to any site where you want to create an account. Click the password text box and you will see "Use suggested password" with a machine-generated one.

If this does not happen, right-click the password text box. Click on "Suggest Password". Google will save the password automatically for future use.

In Chrome's Settings, go to "Safety check". Then tap on "Check Now". Chrome will detect all your weak passwords and prompt you to change them. Take some time every month to review and generate new passwords. Believe me, it is worth it.

18 Jun 2021

14 NIST charts course towards more secure supply chains for government software

by Adam Bannister

https://portswigger.net/daily-swig/nist-charts-course-towards-more-secure-supply-chains-for-government-software

The US NIST has shared a raft of recommendations, submitted by the infosec industry, for bolstering federal agencies' defenses against the burgeoning threat of software supply chain attacks.

NIST is collating suggestions from various tech and infosec organizations with the objective of creating standards and guidelines that will guide the federal government's approach to software procurement and security.

As directed by a recent executive order from President Biden, NIST held a virtual workshop with 1,400 attendees earlier this month, and published 150 papers of recommendations submitted from the likes of Microsoft, Google, and The Linux Foundation.

The announcement comes in the wake of a string of high profile supply chain attacks, such as those against **SolarWinds** and **Codecov** applications, and a deluge of malicious packages that infiltrated open source repositories through 'dependency confusion' in March.

Defining 'critical'

As part of the cybersecurity-focused May directive focused on supply chains, the Biden administration called for "more rigorous and predictable mechanisms" for securing "critical" software, in particular.

However, industry feedback suggests that even defining 'critical' will be challenging.

In its response to NIST's call for papers, for instance, the Software Engineering Institute (SEI) said "software and its context of use are inseparable for the purposes of determining the 'critical' designation".

Citing use cases for OpenSSH, it added: "A hobbyist web server hosting cat pictures and a nuclear power plant have different '... potential for harm if compromised'."

The SEI also warned against adopting a "static" definition for critical software, instead recommending a designation "mechanism" supported by an adapted Stakeholder-Specific Vulnerability Categorization (SSVC).

SALSA

Part of Google's contribution, meanwhile, was an end-to-end framework, called Supply chain Levels for Software Artifacts (SLSA), designed to protect "the integrity of software artifacts throughout the software supply chain".

The tech giant has pitched SLSA as the first framework of its kind to encompass the full development workflow: source-build-publish.

Pronounced 'Salsa', the framework comprises "incrementally adoptable security guidelines" across four levels – ranging from an automated, provenance-generating build process (SLSA 1) through to a two-person review of changes and "a hermetic, reproducible build process" (SLSA 4).

Less is more

The SEI also suggested that federal agencies should expect to see vulnerability disclosure programs (VDP) and software bills of materials (SBOM) on offer from prospective suppliers.

They should also heed the axiom that 'less is sometimes more', suggested the SEI: "operating less software and enabling fewer features reduces attack surface", it said.

Vendors were advised to give appropriate notice of end-of-support dates and "proactively mitigate the risk associated with a single, centralized secure [software] update mechanism" – the attack vector at play in both the SolarWinds and NotPetya attacks.

Existing guidance on these and other areas, added the SEI, was too profuse and ought to be consolidated.

On the subject of testing source code, NIST's workshop summary put forward a recommendation that at least one developer per project "should have security training: specifically, a course where they had to break into a program".

As for choosing tools and technologies, it was suggested that developers use fuzzing as a cost-effective means to pick up elusive, "bizarre cases" of potential vulnerabilities.

According to Brian Fox, co-founder and CTO at DevOps automation platform Sonatype, "the NIST proposal is focused on defining minimum requirements for software sold to the government. These requirements will inevitably influence the rest of the industry given the wide scope of software sold to the US government.

"The Google proposal, on the other hand, goes beyond minimum requirements and proposes a specific model for scoring the supply chain posture that produced a given component," Fox tells The Daily Swig. "Those scores will drive people to focus on many key elements that are often ignored such as 'is the system that built this binary secure?'.

"In summary, NIST is currently focused on 'what' and Google along with other industry proposals are grappling with 'how'."

17 Jun 2021

15 New invention keeps qubits of light stable at room temperature

by University of Copenhagen

https://www.sciencedaily.com/releases/2021/06/210617082723.htm

As almost all our private information is digitalized, it is increasingly important that we find ways to protect our data and ourselves from being hacked.

Quantum Cryptography is the researchers' answer to this problem, and more specifically a certain kind of qubit – consisting of single photons: particles of light.

Single photons or qubits of light, as they are also called, are extremely difficult to hack.

However, in order for these qubits of light to be stable and work properly they need to be stored at temperatures close to absolute zero – that is minus 270 C – something that requires huge amounts of power and resources.

Yet in a recently published study, researchers from University of Copenhagen, demonstrate a new way to store these qubits at room temperature for a hundred times longer than ever shown before.

"We have developed a special coating for our memory chips that helps the quantum bits of light to be identical and stable while being in room temperature. In addition, our new method enables us to store the qubits for a much longer time, which is milliseconds instead of microseconds – something that has not been possible before. We are really excited about it," says Eugene Simon Polzik, professor in quantum optics at the Niels Bohr Institute.

The special coating of the memory chips makes it much easier to store the qubits of light without big freezers, which are troublesome to operate and require a lot of power.

Therefore, the new invention will be cheaper and more compatible with the demands of the industry in the future.

"The advantage of storing these qubits at room temperature is that it does not require liquid helium or complex laser-systems for cooling. Also it is a much more simple technology that can be implemented more easily in a future quantum internet," says Karsten Dideriksen, a UCPH-PhD on the project.

A special coating keeps the qubits stable

Normally warm temperatures disturb the energy of each quantum bit of light.

"In our memory chips, thousands of atoms are flying around emitting photons also known as qubits of light. When the atoms are exposed to heat, they start moving faster and collide with one another and

with the walls of the chip. This leads them to emit photons that are very different from each other. But we need them to be exactly the same in order to use them for safe communication in the future," explains Eugene Polzik and adds:

"That is why we have developed a method that protects the atomic memory with the special coating for the inside of the memory chips. The coating consists of paraffin that has a wax like structure and it works by softening the collision of the atoms, making the emitted photons or qubits identical and stable. Also we used special filters to make sure that only identical photons were extracted from the memory chips."

Even though the new discovery is a breakthrough in quantum research, it stills needs more work.

"Right now we produce the qubits of light at a low rate – one photon per second, while cooled systems can produce millions in the same amount of time. But we believe there are important advantages to this new technology and that we can overcome this challenge in time," Eugene concludes.

16 Are your cryptographic keys truly safe? Root of Trust redefined for the cloud era

by Oded Hareven

https://www.helpnetsecurity.com/2021/06/17/cryptographic-keys-safe/

In the digital world, cryptographic solutions use encryption keys to secure data at rest, data in use, and data in transit. They are responsible for encrypting and decrypting the data, validating identities by authenticating users and devices, and securing transactions with digital signatures and certificates.

Beneath the complex world of encryption use cases and algorithms lies a simple, fundamental principle: the encryption keys must remain a secret. As soon as an encryption key becomes known, it is worthless.

Now, you can and should encrypt the keys themselves, but then how do you protect those encryption keys? This cycle eventually ends with a root key, which is the most important key in the chain. You need to protect your root keys in such a way that you have the highest level of confidence that they will never be compromised – this means you need a Root of Trust.

To further complicate matters, in more secure environments, you might need multiple root keys, for example for different business units or per applications, to mitigate the damage if any single key is exposed.

For years we have assumed that hardware is less vulnerable to attack than software. The resulting consensus is that for the best possible protection you should store encryption keys on hardware, such as on a Hardware Security Module (HSM). HSMs come in the form of USBs, extension cards, and even whole appliances in your data center. You can even rent an HSM on a public cloud.

Is a hardware Root of Trust still the best solution?

Technology has evolved dramatically over the last few years. Driven by the availability of ephemeral infrastructure in the cloud that provides almost unlimited auto-scaling, compute power has increased exponentially. As a by-product of the trend towards cloud computing, the concept of a single, well-defined security perimeter has been virtually obliterated.

The facts on the ground and in the cloud have changed. What does this mean for Root of Trust?

Hardware is no longer invincible

Hardware is not as impenetrable as it used to be. As computing has become more powerful and sophisticated, new hardware attack vectors like Meltdown and Spectre have been discovered that exploit microprocessor vulnerabilities to access data. Even HSMs have been hacked.

Intel's Software Guard Extensions (SGX) provides an alternative approach that enables a CPU to encrypt data in an enclave, which is an isolated environment inside memory. This effectively puts an HSM in every CPU. Unfortunately, SGX has also fallen victim to multiple attacks.

Auto-scaling is a necessity

Modern computing, both within a public or private cloud, is characterized by efficiency, agility, and scalability. This is primarily enabled by software that provides auto-scaling solutions using ephemeral resources.

HSMs are not designed to auto-scale or to be used with a pay-per-use model. You can't automatically spin up another HSM to meet peak demand. Consider a major online retailer who needs X HSMs to validate payment transactions on an ongoing basis, and 3X HSMs to do this over a peak period like Black Friday. The retailer would have to maintain all 3X HSMs year-round, even though they are only required for a couple of days. Similarly, if demand suddenly rises beyond the planned capacity, the retailer will not be able to process payments, potentially losing huge amounts of revenue.

Accessibility is everything

A large and growing number of organizations use distributed hybrid environments, with some resources on-premises and others in the public cloud, in some cases even across multiple regions and multiple clouds. When your resources are everywhere, your Root of Trust needs to be accessible from everywhere too.

If you use an HSM on-premises, you need to provide network access and authentication for cloud resources. This means exposing your internal environment to incoming traffic from external public networks.

Solutions that replicate an on-premises HSM to a CloudHSM attempt to resolve this issue, but these are cumbersome to administer, and although they do resolve the issue of providing access to cloud resources, the issue of authenticating these resources remains.

You're not the exclusive owner of your cloud-based HSM

When you are working with cloud infrastructure, the hardware (and in many cases also the software) is not under your control. This is also true of cloud-based HSMs provided by cloud service providers (CSPs).

You need to look no further than the CLOUD Act to realize that your CSPs have immediate access to your keys and data. This is not theoretical access – this report published by Amazon details the law enforcement data requests with which Amazon complied over a six month period in 2020. It's not a big jump to imagine an insider at your CSP exploiting this ability to expose your keys.

While CSPs make genuine efforts to secure their hardware under the Shared Responsibility Model, the nature of the beast is that using third-party infrastructure also leaves you vulnerable to supply chain attacks. Consider the attack on SolarWinds and imagine the repercussions of your CSP – and by extension you – falling victim to such a large-scale supply chain attack.

Next-gen Root of Trust requirements

It's clear that the implementation of Root of Trust as a purely hardware solution deployed in a single location needs to move with the times. Hardware-based Root of Trust was designed for a different world, and it struggles to meet the demands of modern computing.

We need new solutions that overcome the drawbacks of hardware-only solutions, without compromising security. Essentially, we are looking for solutions that provide true Root of Trust-as-a-service, including:

- Auto-scalability and efficiency, with new models of consumption per transaction, just like any other service. The solution needs to seamlessly grow together with your environment.
- Anytime, anywhere access, whether from on-premises or from the cloud, with omnichannel authentication based on modern authentication methods such as AWS-IAM Roles, Azure Identity, OpenID, and so on.
- Exclusive ownership of your encryption keys and signing keys. Especially in non-trusted environments, the solution needs to guarantee that you are the only party that can access your keys, to ensure they are protected from being exposed to anyone, from federal authorities to malicious attackers.
- International security standard certification, such as US NIST FIPS 140.2. FIPS has several levels of strength. For example, in highly regulated environments, hardware is required to achieve certain FIPS levels, so the solution must be able to include hardware in a scalable way.

17 Bombshell Report Finds Phone Network Encryption Was Deliberately Weakened

by Lorenzo Franceschi-Bicchiera

https://www.vice.com/en/article/4avnan/bombshell-report-finds-phone-network-encryption-was-deliberately-weakened

A weakness in the algorithm used to encrypt cellphone data in the 1990s and 2000s allowed hackers to spy on some internet traffic, according to a new research paper.

The paper has sent shockwaves through the encryption community because of what it implies: The researchers believe that the mathematical probability of the weakness being introduced on accident is extremely low. Thus, they speculate that a weakness was intentionally put into the algorithm. After the paper was published, the group that designed the algorithm confirmed this was the case.

Researchers from several universities in Europe found that the encryption algorithm GEA-1, which was used in cellphones when the industry adopted GPRS standards in 2G networks, was intentionally designed to include a weakness that at least one cryptography expert sees as a backdoor. The researchers said they obtained two encryption algorithms, GEA-1 and GEA-2, which are proprietary and thus not public, "from a source." They then analyzed them and realized they were vulnerable to attacks that allowed for decryption of all traffic.

When trying to reverse-engineer the algorithm, the researchers wrote that (to simplify), they tried to design a similar encryption algorithm using a random number generator often used in cryptography and never came close to creating an encryption scheme as weak as the one actually used: "In a million tries we

never even got close to such a weak instance," they wrote. "This implies that the weakness in GEA-1 is unlikely to occur by chance, indicating that the security level of 40 bits is due to export regulations."

Researchers dubbed the attack "divide-and-conquer," and said it was "rather straightforward." In short, the attack allows someone who can intercept cellphone data traffic to recover the key used to encrypt the data and then decrypt all traffic. The weakness in GEA-1, the oldest algorithm developed in 1998, is that it provides only 40-bit security. That's what allows an attacker to get the key and decrypt all traffic, according to the researchers.

A spokesperson for the organization that designed the GEA-1 algorithm, the European Telecommunications Standards Institute (ETSI), admitted that the algorithm contained a weakness, but said it was introduced because the export regulations at the time did not allow for stronger encryption.

"We followed regulations: we followed export control regulations that limited the strength of GEA-1," a spokesperson for ETSI told Motherboard in an email.

Håvard Raddum, one of the researchers who worked on the paper, summed up the implications of this decision in an email to Motherboard.

"To meet political requirements, millions of users were apparently poorly protected while surfing for years," he said.

Raddum and his colleagues found that GEA-1's successor, GEA-2 did not contain the same weakness. In fact, the ETSI spokesperson said that when they introduced GEA-2 the export controls had been eased. Still, the researchers were able to decrypt traffic protected by GEA-2 as well with a more technical attack, and concluded that GEA-2 "does not offer a high enough security level for today's standards," as they wrote in their paper.

Lukasz Olejnik, an independent cybersecurity researcher and consultant who holds a computer science PhD from INRIA, told Motherboard that "this technical analysis is sound, and the conclusions as to the intentional weakening of the algorithm rather serious."

The good news is that GEA-1 and GEA-2 are not widely used anymore after cellphone providers adopted new standards for 3G and 4G networks. The bad news is that even though ETSI prohibited network operators from using GEA-1 in 2013, the researchers say that both GEA-1 and GEA-2 persist to this day because GPRS is still used as a fallback in certain countries and networks.

"In most countries, [the risk is] not very high, and significantly lower risk than at the start of the 2000's since GEA-3 and GEA-4 are used today," Raddum said. "But handsets still support GEA-1. Scenarios where a mobile phone today can be tricked into using GEA-1 exist."

Phone	Year	Baseband	GEA-1	GEA-2
Apple iPhone XR	2018	Intel XMM 7560	●	●
Apple iPhone 8	2017	Intel XMM 7480	●	●
Samsung Galaxy S9	2018	Samsung Exynos 9810	●	●
HMD Global Nokia 3.1	2018	Mediatek MT6750	●	●
Huawei P9 lite	2016	HiSilicon Kirin 650	●	●
OnePlus 6T	2018	Qualcomm Snapdragon 845	●	●

In fact, the researchers tested several modern phones to see if they would still support the vulner-

able algorithms and "surprisingly" found that they still do. The researchers said that it's the baseband manufacturers who are responsible for implementing standards.

"The use of GEA-1 has still far-reaching consequences on the user's privacy," the researchers wrote, "and should be avoided at all costs."

16 Jun 2021

18 CommStar announces built-in quantum encryption for new satellite links

by Alan Burkitt-Gray

https://www.capacitymedia.com/articles/3828849/commstar-announces-built-in-quantum-encryption-for-new-satellite-links

A new satellite communications project is to use quantum encryption from the start, to protect customers' data.

CommStar Space Communications, which plans to launch its first satellite, CommStar-1, before 2023, has teamed with Quantum Xchange to provide quantum-safe encryption across the network.

But the technology will also be usable over fibre, 4G, 5G or copper, said the company, though its focus at the moment is on satellite services.

"We welcome Quantum Xchange as a new service provider in the CommStar ecosystem and our mission is to transform space communications by 2023," said Fletcher Brumley, CEO of CommStar Space Communications.

CommStar will be unusual in that it will operate between the Earth and the Moon, and it is seen as likely to play a vital role in Nasa's mission to land astronauts on the Moon's surface for the first time since the 1970s.

CommStar has identified Lumen, Orange and Equinix as its partners in providing services.

Brumley said: "With the launch of our hybrid data relay satellite, CommStar-1, and through our work with leading service providers like Quantum Xchange, we can offer customers a highly secure, always-on communications network from and between cislunar, the Moon and Earth."

He is the son of Bob Brumley, head of Laser Light, another advanced communications project, planning to use a combination of satellites and fibre.

"This next-generation space communications network requires equally powerful and innovative next-generation security technologies," said the younger Brumley.

Quantum Xchange's Phio Trusted Xchange (Phio TX) will use an extra layer of encryption, said the company. It "is a simple architecture overlay that leverages an out-of-band symmetric key delivery technology to supplement native encryption with an additional key-encrypting-key (KEK) transmitted independent of the data path and through a quantum-protected tunnel."

CommStar said the "converged global infrastructure and comprehensive services offerings of its service partners will enable the origination, storage, and delivery of space data for use by commercial, civil science, and government entities over an ultra-secure, quantum-protected network".

19 From Scalpels to Qubits: The Story of the World's First Post Quantum Block Chain

by John Potter

https://finance.yahoo.com/news/scalpels-qubits-story-worlds-first-131800504.html?guccounter=1&guce_referrer=aHR0cHM6Ly9uZXdzLmdvb2dsZS5jb20v&guce_referrer_sig=AQAAAGggJ8Z4aC5l5BaZobuhUAwP15rAMAQUdY6MKUnseg8EX17y-DvzURTnyMKcKbenQJWc1zIbvQhLUBeCpBf5ClD1Z1TcYRfCU7FCdJe-wpHW5a_L5BLe-TBAYbJ66n2ZcojsfHJF8ZGsheVUA9T6h14tuHZOY1-Ep9JMW9vkHTSX

For more than a decade, Peter Waterland diligently pursued his role of a surgeon. At the same time, he began delving into a variety of intellectual activities (so much so that he gained a reputation as a polymath). Among these were cryptography, programming and blockchain technology, all of which propelled him to become a passionate cryptocurrency champion.

Peter greatly enjoyed the challenges this new technology presented and made several contributions to the cryptocurrency world as a result, among them a bitcoin bip38 and bitcoin multi-signature wallet and a bitcoin steganography library.

His writings clearly exhibit this passion, as they cover everything from Ethereum economics, to private key encryption. Not incidentally, private key encryption would become his most vexing concern, as he believed it would eventually prove to be the achilles heel of Bitcoin.

Peter realized that a powerful-enough quantum computer could conceivably undermine the Elliptic Curve Digital Signature Algorithm (ECDSA) used in Bitcoin and other cryptocurrencies. Once achieved, an attacker could reconstitute a user's private key from their public key and access their private funds.

In 2016, however, the idea of a practical quantum computer seemed like science fiction to many in the blockchain space. Quantum computers only existed as a handful of qubits, and IBM was a year away from demonstrating any quantum computing whatsoever.

Peter was convinced that this technology would quickly emerge, however, and that a quantum-proof blockchain would soon be needed.

As he would later assert, "(technological) change comes faster than we expect and often in a non-linear fashion" (The QRL Blog).

Although the threat of quantum computers to the blockchain space appeared distant, several organizations had been preparing for this eventuality.

The first organization to take the quantum threat seriously was PQCRYPTO, a global network of post-quantum cryptographers and related professionals. After ongoing discussions about the threat, the organization recommended **XMSS as a post-quantum security solution** in March 2015. Several months later, the NSA announced that they were preparing for the quantum-threat.

20 Google open-sources tools to bring fully homomorphic encryption into the mainstream

by John Leyden

https://portswigger-net.cdn.ampproject.org/c/s/portswigger.net/daily-swig/amp/google-open-sources-tools-to-bring-fully-homomorphic-encryption-into-the-mainstream

Google has released a set of coding utilities that allow fully homomorphic encryption (FHE) operations on encrypted data.

The open source collection of libraries and tools allow computational processes to be carried out on encrypted data without first having to decrypt it, offering security and privacy benefits as a result.

Homomorphic encryption and secure multi-party computation are known technologies. Google's release is largely focused on refining and making them suitable for wider deployment, rather than reinventing the basis for the technologies.

"Our release focuses most on ease of use, cleanly abstracting the various layers of development between design (what the developer is actually trying to do) and implementation (what actually is performed)," a Google spokesperson told The Daily Swig.

"The transpiler offers a glimpse into all of these layers, allowing the combined expertise of the crypto, hardware, logical optimization and distributed computing communities to come together in one place."

The suite of tools is available on Github.

Use cases: Fully homomorphic encryption

Use cases for homomorphic encryption range from "spell checkers for an email, to updates from wearables, to medical record analysis to, further down the road, things like photo filters or genomic analysis", according to Google.

"The more sensitive or identifying the use case might be, the more important it is that a developer is able to provide strong guarantees on data handling," the Google spokesperson added.

No special expertise in cryptography is required to make use of the search giant's technology, which is geared towards overcoming a lack of crypto expertise amongst developers that has historically held back wider adoption of such tools.

The trade-off for the privacy benefits of homomorphic encryption is that the mechanism can be more computationally intensive and slower than other methods – an issue not immediately addressed in Google's release.

"Performance remains a significant barrier (one we continue to work on) and so this won't be a drop-in replacement for all existing cloud services," the Google representative explained.

"At the moment, this environment is aimed at well-scoped problems where data sensitivity is critical or where extra compute cost is worth the added privacy benefit."

Google's approach to fully homomorphic encryption in explained in more detail in a recent white paper.

Professor Alan Woodward, a computer scientist from the University of Surrey, said Google's FHE tools might be useful across a wide range of applications.

"What Google appear to be doing is providing tools to enable FHE across a wide range of areas," he explained.

"Bottom line is that anything where you want the dataset encrypted when in live use, not just encrypted at rest, then FHE could help."

21 Seeqc and Riverlane Report the Successful Demonstration of a Quantum Operating System Running on a Unique, Chip-scale Integrated Quantum Computing Architecture

by Matt Swayne

https://thequantumdaily.com/2021/06/16/seeqc-and-riverlane-report-the-successful-demonstration-of-a-quantum-operating-system-running-on-a-unique-chip-scale-integrated-qua

A US-UK partnership report in a news release that the successful demonstration of a quantum operating system running on a unique, chip-scale integrated quantum computing architecture represents a key stage in the development a scalable quantum computer.

Seeqc, the Digital Quantum Computing company, has achieved this through a partnership with Riverlane, UK developer of the first universal quantum operating system, Deltaflow.OS. The success represents an important demonstration of the portability of Deltaflow.OS.

"In its most simple terms, we have put something that once filled a room onto a chip the size of a coin, and it works," said Dr. Matthew Hutchings, London-based chief product officer and co-founder of Seeqc.

Tight integration of Deltaflow.OS on Seeqc's platform will enable Seeqc to maximise the low-latency performance available through its chip-scale technology. Low-latency performance is important for running quantum algorithms efficiently and achieving quantum advantage.

Seeqc and Riverlane make up an important part of the UK quantum technology sector, and co-location in the UK is key to achieving tight system integration.

Hutchings said: "This is the first time we have built an integrated quantum computing chip based on our unique scalable architecture and run a program on it. We achieved stability and full-stack control and, in so doing, also a remarkable moment for the evolution of quantum computing."

"This is as significant for the future of quantum computers as the microchip itself was for commercialising traditional computers, allowing them to be produced cost-effectively and at scale," Hutchings continued.

Dr. Steve Brierley, Founder and CEO of Riverlane said: "This successful demonstration of Deltaflow.OS onto Seeqc's hardware is hugely encouraging. By combining quantum hardware and software expertise, we have solved a key challenge in quantum computing; ensuring portability and high performance across different qubit technologies."

This important milestone was achieved by Seeqc's UK team, which is focused on design and system integration. The work was supported by the NISQ.OS Innovate UK grant and achieved using the advanced commercial quantum measurement facilities at QUES2T, operated by University College London. Seeqc is constructing a state-of-the-art lab facility in central London, due for completion in October and designed to support platform product development.

15 Jun 2021

22 Belief propagation with quantum messages for quantum-enhanced classical communications

https://www.nature.com/articles/s41534-021-00422-1

For space-based laser communications, when the mean photon number per received optical pulse is much smaller than one, there is a large gap between communications capacity achievable with a receiver that performs individual pulse-by-pulse detection, and the quantum-optimal "joint-detection receiver" that acts collectively on long codeword-blocks of modulated pulses; an effect often termed "superadditive capacity". In this paper, we consider the simplest scenario where a large superadditive capacity is known: a pure-loss channel with a coherent-state binary phase-shift keyed (BPSK) modulation. The two BPSK states can be mapped conceptually to two non-orthogonal states of a qubit, described by an inner product that is a function of the mean photon number per pulse. Using this map, we derive an explicit construction of the quantum circuit of a joint-detection receiver based on a recent idea of "belief-propagation with quantum messages" (BPQM). We quantify its performance improvement over the Dolinar receiver that performs optimal pulse-by-pulse detection, which represents the best "classical" approach. We analyze the scheme rigorously and show that it achieves the quantum limit of minimum average error probability in discriminating 8 (BPSK) codewords of a length-5 binary linear code with a tree factor graph. Our result suggests that a BPQM receiver might attain the Holevo capacity of this BPSK-modulated pure-loss channel. Moreover, our receiver circuit provides an alternative proposal for a quantum supremacy experiment, targeted at a specific application that can potentially be implemented on a small, special-purpose, photonic quantum computer capable of performing cat-basis universal qubit logic.

23 IBM's Quantum System One comes to Europe

by Katia Moskvitch

https://research.ibm.com/blog/fraunhofer-quantum-system-one

Europe's largest application-oriented research organization Fraunhofer-Gesellschaft received a special multi-package delivery from overseas a few months ago. Inside was an **IBM Quantum System One** – which until now had only existed in IBM's New York-based data center.

Fraunhofer-Gesellschaft is betting that Quantum System One will pave the way to future industrial applications of this new way of computation. It should also lead to ever more research and help develop a global quantum-ready workforce. It's the first step towards commercially scaling IBM's quantum computing technology. In July, a quantum computer in Japan will join its Fraunhofer cousin, and in the not too distant future one will also be installed at Cleveland Clinic in Ohio.

"Quantum computing opens up new possibilities for industry and society," says Hannah Venzl, the coordinator of Fraunhofer Competence Network Quantum Computing. "Drugs and vaccines could be developed more quickly, climate models improved, logistics and transport systems optimized, or new materials better simulated. To make it all happen, to actively shape the rapid development in quantum computing, we need to build up expertise in Europe."

Building up expertise is vital to create a quantum industry. We expect that within the decade, we will achieve a "quantum advantage" – the point when quantum computers will provide more-accurate,

computationally cheaper solutions; or even allow us to calculate solutions to problems we can't solve today. When that happens, these machines are likely to change the world. But the world needs to be ready for them – with a skilled, creative, results-driven talent.

That's our quantum future – and with these machines now starting to pop up across the globe, it may be closer than you think.

Tackling the quantum talent shortage

Fraunhofer's new addition is mirror-black and shiny. Behind the system's giant doors, made of the same glass protecting the Mona Lisa in the Louvre, there is a cylinder-like structure. Inside is the 27-qubit Falcon processor, IBM's most-advanced, hard-tech quantum processor. It's kept at a temperature colder than outer space, with qubits that have long coherence times – how long they remain in their quantum state – and precise, low-noise operations of about 10^{20} watts.

While Fraunhofer is the first place outside the US to have an IBM Quantum System One, the interest in quantum technologies has been steadily growing over the past decade. Nearly all continents now have quantum computing startups, and many tech giants in addition to IBM are making strides in the field. In total, the global market for quantum technologies could soon reach nearly $22 billion.

But here is the thing. While investments in research and the research itself are important, they are not enough. There is a disconnect between the development of a quantum computer and its wide-scale commercialization.

Only a fraction of businesses are getting quantum-ready. The vast majority of companies still do not have the workforce able to use quantum computers, to do any kind of quantum programming, or even have an idea how a quantum computer could help them. There is little on-the-job quantum training and few hires with quantum computing skills.

That's why partnerships like the one between IBM and Fraunhofer are crucial – even though it's not necessary to buy a quantum computer to access one. Currently 150 organizations in IBM's Quantum Network including research labs, start-ups, universities and enterprises access IBM's quantum fleet via the cloud. Still, being able to have the machine on premises helps with processing more data, locally.

Fraunhofer's System One, which came online a few weeks ago for testing, is already hard at work. Focusing on quantum optimization, researchers here in Germany have started exploring new simulation approaches for materials in energy storage systems. Another project being actively studied by the local researchers is to better-optimize financial asset portfolios and improve the stability parameters in energy supply infrastructures. They even aim to use the quantum computer to push the limits of deep learning with quantum machine learning.

"At Fraunhofer, we have more than 70 years of expertise in applied research and industrial projects, and we are closely interlinked with industry," says Venzl. "The training on the system will help us develop practical applications and build up important competencies in German industry and at Fraunhofer itself."

The ball at Fraunhofer is definitely rolling – but getting the machine here was anything but trivial.

24 The Race for Quantum Computing and Cryptography Is Accelerating

by Julianne Simpson

https://www.afcea.org/content/race-quantum-computing-and-cryptography-accelerating

Quantum computing and cryptography are hot topics in the world of emerging technology. But how feasible are they on a large scale?

"Right now those things are energy intensive and expensive and time consuming," said Bill Halal, founder of TechCast, during the virtual AFCEA/GMU C4I Center Symposium.

Peter Fonash, chief technology officer, Option3Ventures, agreed. "I think you have to go look at things in terms of where they are in the lifecycle. If you look at quantum computing, it's still in its early stages. The machines that they've developed are very small and they also require special conditions like special cooling," he said. "The temperature demands of the quantum computers are even more demanding than those old Cray supercomputers."

Quantum is very expensive and is still in its research and development stage, said Fonash. "In fact when you look at how much money is being spent on quantum encryption, in 2019 it was $8 million for the whole year," he said. So far in 2021 it's $30 million. It's an enormous growth but still not in the hundreds of millions, added Fonash.

The National Institute of Standards and Technology (NIST) is also still developing a standard for post quantum encryption. They are scheduled to come up with a standard this year. Fonash estimates quantum is about five years away from wide deployment but, "I think we are in an arms race with China. And that's going to accelerate because of its military implications and from a hacking point of view and also for general communications where you can secure all communications through encryption."

Fonash sees a real use for quantum encryption by the big cloud providers, like Google and Microsoft where you have something like OneDrive. "You could store it on your computer but the cloud would actually encrypt it for you," he explained.

"That could ensure the security of an individual signing into his accounts on the cloud," said Halal, relating it to blockchain.

Fonash certainly sees the potential for blockchain but sees a big challenge in its efficiency. "When you try to scale up a community, it gets very large and it gets very process intense. That's where the work effort is going to be, to make [blockchain] more efficient so that it can scale," said Fonash.

Halal posed the idea that artificial intelligence (AI) could help with efficiency.

"Maybe," said Fonash. "AI has great potential but sometimes human beings can take the time and scratch their heads and say, 'You know I think this is right but it doesn't make sense to me.' There's a sixth sense of a human being, which an AI system may never have. The human being may want to go look at one more thing where as the AI just takes action," explained Fonash.

25 Google Messages end-to-end encryption is now out of beta

by Abner Li

https://9to5google.com/2021/06/15/google-messages-encryption/

Back in November, Google announced that it would start testing end-to-end encryption in Messages for Android. After being limited to the beta channel, E2EE is now rolling out to all stable users.

With end-to-end encryption enabled, Google or other third parties cannot read the contents (text and media) of your RCS chats as it's in transit between the sender and receiver. Google is using the Signal Protocol and offers a technical paper with more details.

E2EE requires both parties to have Chat features and data/Wi-Fi enabled. It does not work for SMS/MMS or group messaging, though it's available when using the Messages for web app. If those requirements are met, this layer of security is automatically active for both existing and new conversations. It cannot be disabled in a privacy-conscious stance by Google.

You will see a lock icon in the "Chatting with" banner, timestamps, and on the send button when end-to-end encryption is enabled/used for delivery. Meanwhile, if E2EE is temporarily lost, the default behavior will be to hold the message until that secure connection is restored, though you can decide to send with SMS.

Encryption converts data into scrambled text that's unreadable without a secret key number that's only available "on your device and the device you message." It's "generated again for each message" and "deleted from the sender's device when the encrypted message is created, and deleted from the receiver's device when the message is decrypted."

Each E2EE conversation also has a unique verification code that you can manually verify with the other person by tapping the overflow menu ¿ Details ¿ Verify encryption.

End-to-end encryption in Google Messages was quietly announced alongside other summer Android announcements today. We've reached out to Google for additional confirmation, but the accompanying support document no longer tells users to sign up for the Messages beta.

14 Jun 2021

26 New combination of materials provides progress toward quantum computing

by Rensselaer Polytechnic Institute

https://www.sciencedaily.com/releases/2021/06/210614153900.htm

The future of quantum computing may depend on the further development and understanding of semiconductor materials known as transition metal dichalcogenides (TMDCs). These atomically thin materials develop unique and useful electrical, mechanical, and optical properties when they are manipulated by pressure, light, or temperature.

In research published today in Nature Communications, engineers from Rensselaer Polytechnic Institute demonstrated how, when the TMDC materials they make are stacked in a particular geometry, the interaction that occurs between particles gives researchers more control over the devices' properties. Specifically, the interaction between electrons becomes so strong that they form a new structure known as a correlated insulating state. This is an important step, researchers said, toward developing quantum emitters needed for future quantum simulation and computing.

"There is something exciting going on," said Sufei Shi, an assistant professor of chemical and biological engineering at Rensselaer, who led this work. "One of the quantum degrees of freedom that we hope to use in quantum computing is enhanced when this correlated state exists."

Much of Shi's research has focused on gaining a better understanding of the potential of the exciton, which is formed when an electron, excited by light, bonds with a hole – a positively charged version of the electron. Shi and his team have demonstrated this phenomenon in TMDC devices made of layers of Tungsten disulfide (WS2) and Tungsten diselenide (WSe2). Recently, the team also observed the creation of an interlayer exciton, which is formed when an electron and hole exist in two different layers of material. The benefit of this type of exciton, Shi said, is that it holds a longer lifetime and responds more significantly to an electric field – giving researchers greater ability to manipulate its properties.

In their latest research, Shi and his team showed how, by stacking TMDCs in a particular manner, they can develop a lattice known as a moiré superlattice. Picture two sheets of paper stacked on top of one another, each with the same pattern of hexagons cut out of them. If you were to shift the angle of one of the pieces of paper, the hexagons would no longer perfectly match up. The new formation is similar to that of a moiré superlattice.

The benefit of such a geometry, Shi said, is that it encourages electrons and interlayer excitons to bond together, further increasing the amount of control researchers have over the excitons themselves. This discovery, Shi said, is an important step toward developing quantum emitters that will be needed for future quantum simulation and quantum computing.

"It has essentially opened the door to a new world. We see a lot of things already, just by peeking through the door, but we have no idea what is going to happen if we open the door and get inside," Shi said. "That is what we want to do, we want to open the door and get inside."

12 Jun 2021

27 The 3rd PQC Standardization Conference

by Luca de Feo

https://ellipticnews.wordpress.com/2021/06/12/report-by-luca-de-feo-on-the-3rd-pqc-standardization-conference/

The 3rd PQC Standardization Conference, organized by NIST, took place online from June 7 to 9, featuring a mix of live talks, pre-recorded talks, and panels. The oral exchanges were complemented by a text-based forum, provided by an app well known for its lack of end-to-end encryption, where some topics were eventually debated at length. Slides for the talks will be available in a few days, and video recordings in a few weeks. In the meantime, I will give a personal account of the conference based exclusively on my recollections. I took no notes, and I was often preparing or eating dinner at the same time, so nothing of what I will report should be taken as an established truth.

Kicking-off the conference, NIST gave some interesting bits of information on the status of the selection process and the future. The timeline for the 3rd round stays put: NIST expects to announce the selected standards sometimes between the end of 2021 and the beginning of 2022, as well as the alternates that will move to Round 4. Two announcements stirred more emotions in the audience: NIST reported on the difficulties of acquiring patents that are perceived to hinder standardization of some candidates, and specifically pointed to a statement recently published by CNRS. Several researchers with links to French

academia have already expressed their disappointment with CNRS' strategy. The second was a confirmation of a possibility that NIST had already hinted at previously: roughly 6 months after the end of the 3rd round, NIST plans to reopen the process to submissions, specifically seeking to add more variety to signatures. The audience understood that NIST will not accept new KEM candidates in this phase. Given the recent progress in designing post-quantum signature schemes, including some that received accolades at AsiaCrypt, this announcement should interest the readers of this blog. In the same spirit, NIST doubled down on the possibility of standardizing SPHINCS+ at the end of the 3rd round.

Throughout the three days, each of the finalists and alternate finalists had a 15 minutes slot to present their updates for the 3rd round. In most cases, there were minimal or no updates. PicNic appears to be the most notable exception, with important changes to the structure of the LowMC block cipher. Rainbow and GeMSS had some explaining to do, in response to recent advances in cryptanalysis, and GeMSS had to drop some parameters. Vadim Lyubashevsky and Dan Bernstein possibly gave the most opinionated talks, I recommend watching both when they are available.

Several contributed talks reported on various aspects of post-quantum cryptography. Lattices had the greatest share, I especially enjoyed the talks by Thomas Espitau and Yu Yang on variants of Falcon ... or maybe was it the excellent Château Latour I was having at the same time? I also enjoyed the "Applications" session, which opened my eyes on how difficult it is to put any of the PQC candidates in constrained environments such as smartcards and IoT.

Of particular interest to the readers of this blog should be the three contributed talks on isogeny-based cryptography:

- Péter Kutas (joint work with Christophe Petit) gave an excellent, if somewhat time-constrained, survey talk on several different "torsion point attacks" against SIDH and variants, which have previously appeared in this blog. The take-away message is that SIDH, SIKE and B-SIDH are well protected against all of them, be it because of the Fujisaki–Okamoto transform, or because of their intrinsic limitations, but the broader space of generalizations of SIDH a cryptographer might imagine is somewhat limited by these attacks, as it has already been repeatedly shown. I would certainly like to see more research in this promising direction, which has applications beyond cryptanalysis.
- Élise Tasso (joint work with Nadia El Mrabet, Simon Pontié and myself) presented an in-the-lab confirmation of a fault-injection attack on SIDH first proposed by Ti. The attack is alarmingly easy to mount (ok, we used equipment worth 40k€, but that's only because we're rich), but at the same time:
  - It requires multiple repetitions of key generation with the same secret key, something that should never happen in a correct implementation of SIDH or SIKE;
  - It appears to be difficult to exploit in presence of key compression;
  - It has a countermeasure so simple and cheap, that it may as well be included by default in the reference code.

The old-timers of this blog will not be surprised to learn that the best talk of the conference was delivered by Craig Costello. In only 5 minutes, Craig pretended **to use SageMath code to generate pairs of toy SIDH public keys** (one for Alice, one for Bob), discard the secrets, and (clumsily fail to) upload the public keys to a GitHub repo. Then, he announced that Microsoft is offering \$5,000 for the solution of the smaller instance, named \$IKEp182, and \$50,000 for that of the larger instance, named

$IKEp217. The prize money matches what the SIKE team estimates to be the material cost of breaking the instances, so think twice before reallocating your BitCoin mining resources.

11 Jun 2021

28 Quantum encryption via satellite

by David Manners

https://www.electronicsweekly.com/news/business/quantum-encryption-via-satellite-2021-06/

The UK, USA, Japan, Canada, Italy, Belgium and Austria are now represented.

Arqit's system uses satellites to distribute quantum keys to data centres. These keys are delivered using a protocol called ARQ19, which solves the "Global versus Trustless" problem which previously prevented the adoption of Satellite Quantum Key Distribution (QKD).

Arqit invented a method, called **QuantumCloud** to translate the benefits of this quantum key distribution to any form of endpoint or cloud machine without the need for any special hardware. The first version of QuantumCloud launches for live service to commercial customers in 2021.

Government customers typically have more stringent requirements for control and are more inclined to buy "Private Instances" of cloud technology rather than managed services.

Arqit has therefore designed a different version of its technology to meet this need and has recruited a partners from allied countries to collaborate in bringing the FQS system to use.

Collaboration partners include BT, Sumitomo Corporation, Northrop Grumman, Leonardo, QinetiQ Space N.V., qtlabs and Honeywell. Other Western Allied countries are expected to announce their inclusion during 2021.

FQS has been developed with support from the UK Space Agency (UKSA through its National Space Innovation Programme). The system consists of dedicated satellites, control systems and QuantumCloud software.

It will be provided to the UK's 'Five Eyes' allied governments and other international partners, allowing sovereign protection of strategic national assets and interoperability for joint operations.

The first FQS satellites are to be integrated and tested at the National Satellite Test Facility in Harwell near Oxford and are expected to be launched on Virgin Orbit's LauncherOne from Newquay in Cornwall in 2023, after the launch of the first commercial Arqit satellites.

29 Governments ally for federated quantum encryption satellite network

by Sophia Chen

https://spacenews.com/governments-ally-for-federated-quantum-encryption-satellite-network/

The United States and five other countries are banding together with the United Kingdom to develop a satellite-based quantum technology encryption network.

The Federated Quantum System (FQS) will be based on the one British startup Arqit is developing for commercial customers, using quantum technology breakthroughs to guard against increasingly sophisticated cyberattacks.

But while that network is on a managed services platform run by Arqit, FQS will be closed off in a way that enables interoperability between allied countries.

Fighter jets and other military units and command and control centers would be able to share communications more securely across a sovereign-controlled network.

The governments of Japan, Canada, Italy, Belgium and Austria are also partnering on the initiative, which includes companies from each country to design and test the system.

Those commercial partners include British telco BT, U.S. aerospace giant Northrop Grumman, Japanese investment firm Sumitomo, Italian technology group Leonardo and Austrian quantum technology startup QTL.

The Canadian and Belgian subsidiaries of aerospace company Honeywell and defense technology firm Qinetiq, respectively, have also joined.

The cost of the project including an initial satellite in 2023 is expected to be more than $70 million, funded by the consortium's government and commercial partners.

They will also have the option to buy a dedicated version at a cost of around $250 million over 10 years.

Arqit is lining up Virgin Orbit to launch the first FQS satellites in 2023 from the U.K., after it orbits a pair of spacecraft for its commercial counterpart that year.

Virgin Orbit, an air-launched rocket startup nearing the launch of its first payload for commercial customers, earlier invested in Arqit as part of the quantum venture's merger with a special purpose acquisition company (SPAC).

Arqit expects to raise $400 million from that deal once it closes in the third quarter of this year.

The startup plans to make the first version of its QuantumCloud software available in July.

The software generates an unlimited number of encryption keys at the end point of customer devices, and will rely on terrestrial communications until its satellites are launched.

Arqit says using quantum computing technology for symmetric encryption is more secure than systems based on public key infrastructure (PKI), which is used to encrypt most of the world's communications.

Another conflict?

It is unclear what the European Union will make of Italy, Belgium and Austria's participation in Arqit's FQS.

The three countries – and all EU members apart from Ireland – have signed up to plans to develop a European quantum communications network called EuroQCI.

Airbus said May 31 it secured a contract from the European Commission to lead a consortium to study the quantum technology-powered network for Europe.

Leonardo is part of the 15-month study group, along with accountancy firm PwC France and Maghreb, French telecoms giant Orange and Italy's CNR research council and NRiM meteorological institute.

Telespazio, a joint venture between Leonardo and French aerospace group Thales, is also part of the group.

An EU official recently suggested there may be a conflict of interest arising from French satellite operator Eutelsat's $500 million investment in OneWeb in April.

Eutelsat is part of a separate consortium that has been studying a new satellite broadband constellation for the European Union since December.

30 The race is on for quantum-safe cryptography

by Sophia Chen

https://www.theverge.com/22523067/nist-challenge-quantum-safe-cryptography-computer-lattice

In 2016, Lily Chen started a competition to rewrite the building blocks of encryption.

With her team of mathematicians at the US National Institute of Standards and Technology, Chen reached out to academic and industry cryptographers around the world to find algorithms that could resist new threats posed by quantum computers. Five years later, the project is almost complete. After three rounds of elimination, Chen and her team have now narrowed the 69 submissions down to a final seven algorithms, with several winners to be named at the end of the year. If things go according to plan, the result will be a new set of NIST-certified algorithms – and a new measure of protection against the chaos of a fully operational quantum computer.

"Cryptosystems in devices and communication systems will not be secure anymore" when those computers reach their potential, Chen says. "It's time to prepare for quantum threats."

Chen has technical reasons to be concerned. Existing encryption systems rely on specific mathematical equations that classical computers aren't very good at solving – but quantum computers may breeze through them. As a security researcher, Chen is particularly interested in quantum computing's ability to solve two types of math problems: factoring large numbers and solving discrete logarithms (essentially solving the problem $b^x = a$ for x). Pretty much all internet security relies on this math to encrypt information or authenticate users in protocols such as Transport Layer Security. These math problems are simple to perform in one direction, but difficult in reverse, and thus ideal for a cryptographic scheme.

"From a classical computer's point of view, these are hard problems," says Chen. "However, they are not too hard for quantum computers."

In 1994, the mathematician Peter Shor outlined in a paper how a future quantum computer could solve both the factoring and discrete logarithm problems, but engineers are still struggling to make quantum systems work in practice. While several companies like Google and IBM, along with startups such as IonQ and Xanadu, have built small prototypes, these devices cannot perform consistently, and they have not conclusively completed any useful task beyond what the best conventional computers can achieve. In 2019, Google reported that its quantum computer had solved a problem faster than the best existing supercomputers, but it was a contrived task with no practical application. And in 2020, academic researchers in China also reported their quantum computer had beat conventional computing in performing an algorithm that could offer utility for specialized optimization tasks. But so far, quantum computers have only managed to factor tiny numbers like 15 and 21 – a useful proof of principle, but far from a practical threat.

That hasn't stopped researchers from trying to stay one step ahead of the quantum challenge. Peter Schwabe, a mathematician at the Max Planck Institute for Security and Privacy, has devised several cryptography schemes with colleagues that have beat the third round of NIST's competition. One of his

submissions qualifies as a lattice-based protocol, a class of quantum-resistant algorithms that involve a geometric puzzle in a grid of points, arranged across hundreds or even thousands of dimensions. To crack the code, the computer must use given line segments to solve the puzzle, such as finding the most compact way to connect the lines end to end in the grid.

"**Lattice-based cryptography** is, at the moment, considered the most realistic drop-in replacement for the protocols we have today," says Schwabe.

It's important to establish cryptographic standards now because once NIST standardizes a new cryptographic protocol, it will take years for some users to buy and set up the necessary technology. Another worry is that hackers today could intercept and store encrypted information, and then decrypt the messages a decade later with a quantum computer. This is a particular concern for government agencies that create documents intended to remain classified for years.

"We have to try and get these cryptosystems ready well in advance of quantum computers," says NIST mathematician Dustin Moody, a member of Chen's team.

In advance of NIST's standards, some companies have already begun experimenting with these new cryptography schemes. In 2019, Google and the security company Cloudflare began testing the speed and security of two quantum computing-resistant protocols. "We hope that this experiment helps choose an algorithm with the best characteristics for the future of the internet," wrote cryptographer Kris Kwiatkowski of Cloudflare in a blog post after the tests were performed.

When the winning algorithms are chosen, the hope is that NIST's federal certification will spur more companies to follow suit, and give them a head start in testing and implementing quantum-safe cryptography. Ultimately, NIST researchers see this work as public service. They aim to make these cryptographic standards freely available. The agency doesn't pay cryptographers to participate in the competition, and winners will not receive any money. "You just get fame in the cryptographic world, which carries its own weight," says Moody.

And the winners get the satisfaction of knowing they've completely redesigned swaths of internet infrastructure. The new protocols will alter fundamental interactions on the internet, like how your computer confirms you've actually accessed the right website and not a hacker's server – not to mention how companies encrypt your credit card number when you make an online purchase.

But the revolution will be quiet. "The average user is not really going to see or notice this," says Moody. "Hopefully, it'll all be done behind the scenes by the cryptographers and the people who put this into their products." Like the best security products, you can tell it's working when nobody notices the change.

10 Jun 2021

31 IonQ Adds Integration with Google Cirq, Making IonQ's Leading Systems Operable with all Major Quantum Software Frameworks

https://ionq.com/news/june-10-2021-2021-06-10-ionq-adds-integration-with-google-cirq

IonQ, Inc., the leader in trapped-ion quantum computing, today announced the full integration of its quantum computing platform with **Cirq**, a leading open-source quantum computing framework from Google. Volkswagen Group has already run the "paint shop problem" on IonQ via Cirq and found the performance to be consistent with other quantum software frameworks.

"From its origins, the vision for Cirq was to expand access to quantum computing to even broader audiences," said Dave Bacon, VP of Software at IonQ (and one of the original authors of Cirq). "As a developer myself, I know that a smoother, simpler implementation is a better implementation, one that will be more useful in the real world. Volkswagen has shown that developing in Cirq on IonQ has real benefits for real problems faced by development teams."

For Volkswagen, running the "paint shop problem" is a useful benchmark because it is a sequential ordering challenge reflective of many of the industry problems they hope quantum computing will help address. Cirq is fast and simple to deploy, and Volkswagen found that running on IonQ via Cirq produced the same results as doing so via other quantum frameworks.

"Applied quantum computing is still in its infancy, and the easier it becomes to access quantum computing hardware like IonQ's via different tools, the broader and faster the adoption across many industries," said Dr. Florian Neukart, Director, Volkswagen Data Lab. "This will speed up the development of industry-relevant applications, which is also what we focus on at Volkswagen."

"It's great to see the adoption of Cirq following the spirit of the Apache 2.0 open source license and making further hardware platforms accessible to the global Cirq developer community. It's even nicer to see this integration immediately being adopted by our collaborators from Volkswagen in such a great Cirq tutorial," explains Dr. Markus Hoffmann, Quantum Partnerships at Google Quantum AI.

Realizing the world-changing promise of quantum computing will require open, interoperable systems that enable users from academia, industry, and commerce to quickly access quantum hardware. By integrating with Cirq, and supporting all major quantum language and software frameworks, IonQ is further lowering barriers to entry by researchers, developers, and innovators. Cirq users, as well as users of all other major quantum SDKs, including Qiskit, PennyLane, Orquestra, Strangeworks QC and more can now submit programs to IonQ's platform without writing any new code.

This integration with Google Cirq builds on IonQ's continued success and proven performance. The company's 11-qubit system is the first and only quantum computer available via the cloud on Amazon Braket and Microsoft Azure, and its 32-qubit system is one of the world's most powerful quantum computers. IonQ has a critical role to play in pulling the quantum computing industry forward as its plans to develop modular quantum computers small enough to be networked together in 2023 could pave the way for broad quantum advantage by 2025, and its two co-founders, Jungsang Kim and Chris Monroe, were named to the White House's National Quantum Initiative Advisory Committee (NQIAC). IonQ will further expand access to quantum as it prepares to become the first publicly traded quantum computing company via a merger with dMY Technology Group III.

32 Researchers create an 'un-hackable' quantum network over hundreds of kilometers using optical fiber

by Daphne Leprince-Ringuet

https://www.zdnet.com/article/researchers-created-an-un-hackable-quantum-network-over-hundreds-of-kilometers-using-optical-fiber/

Researchers from Toshiba have successfully sent quantum information over 600-kilometer-long optical fibers, creating a new distance record and paving the way for large-scale quantum networks that could be used to exchange information securely between cities and even countries.

Working from the company's R&D lab in Cambridge in the UK, the scientists demonstrated that they could transmit quantum bits (or qubits) over hundreds of kilometers of optical fiber without scrambling the fragile quantum data encoded in the particles, thanks to a new technology that stabilizes the environmental fluctuations occurring in the fiber.

This could go a long way in helping to create a next-generation quantum internet that scientists hope will one day span global distances.

The quantum internet, which will take the shape of a global network of quantum devices connected by long-distance quantum communication links, is expected to enable use-cases that are impossible with today's web applications. They range from generating virtually un-hackable communications, to creating clusters of inter-connected quantum devices that together could surpass the compute power of classical devices.

But in order to communicate, quantum devices need to send and receive qubits – tiny particles that exist in a special, but extremely fragile, quantum state. Finding the best way to transmit qubits without having them fall from their quantum state has got scientists around the world scratching their heads for many years.

One approach consists of shooting qubits down optical fibers that connect quantum devices. The method has been successful but is limited in scale: small changes in the environment, such as temperature fluctuations, cause the fibers to expand and contract, and risk messing with the qubits.

This is why experiments with optical fiber, until now, have typically been limited to a range of hundreds of kilometers; in other words, nowhere near enough to create the large-scale, global quantum internet dreamed up by scientists.

To tackle the instable conditions inside optical fibers, Toshiba's researchers developed a new technique called "dual band stabilization". The method sends two signals down the optical fiber at different wavelengths. The first wavelength is used to cancel out rapidly varying fluctuations, while the second wavelength, which is at the same wavelength as the qubits, is used for finer adjustments of the phase.

Put simply, the two wavelengths combine to cancel environmental fluctuations inside the fiber in real time, which according to Toshiba's researchers, enabled qubits to travel safely over 600 kilometers.

Already, the company's team has used the technology to trial one of the most well-known applications of quantum networks: quantum-based encryption.

Known as Quantum Key Distribution (QKD), the protocol leverages quantum networks to create security keys that are impossible to hack, meaning that users can securely exchange confidential information, like bank statements or health records, over an untrusted communication channel such as the internet.

During a communication, QKD works by having one of the two parties encrypt a piece of data by encoding the cryptography key onto qubits and sending those qubits over to the other person thanks to a quantum network. Because of the laws of quantum mechanics, however, it is impossible for a spy to intercept the qubits without leaving a sign of eavesdropping that can be seen by the users – who, in turn, can take steps to protect the information.

Unlike classical cryptography, therefore, QKD does not rely on the mathematical complexity of solving security keys, but rather leverages the laws of physics. This means that even the most powerful computers would be unable to hack the qubits-based keys. It is easy to see why the idea is gathering the attention of players from all parts, ranging from financial institutions to intelligence agencies.

Toshiba's new technique to reduce fluctuations in optical fibers enabled the researchers to carry out

QKD over a much larger distance than previously possible. “This is a very exciting result,” said Mirko Pittaluga, research scientist at Toshiba Europe. “With the new techniques we have developed, further extensions of the communication distance for QKD are still possible and our solutions can also be applied to other quantum communications protocols and applications.”

When it comes to carrying out QKD using optical fiber, Toshiba’s 600-kilometer mark is a record-breaker, which the company predicts will enable secure links to be created between cities like London, Paris, Brussels, Amsterdam and Dublin.

Other research groups, however, have focused on different methods to transmit qubits, which have enabled QKD to happen over even larger distances. Chinese scientists, for example, are using a mix of satellite-based transmissions communicating with optical fibers on the ground, and recently succeeded in carrying out QKD over a total distance of 4,600 kilometers.

Every approach has its pros and cons: using satellite technologies is more costly and could be harder to scale up. But one thing is certain: research groups in the UK, China and the US are experimenting at pace to make quantum networks become a reality.

Toshiba’s research was partially funded by the EU, which is showing a keen interest in developing quantum communications. Meanwhile, China’s latest five-year plan also allocates a special place for quantum networks; and the US recently published a blueprint laying out a step-by-step guide leading to the establishment of a global quantum internet.

09 Jun 2021

33 Qrypt Makes First Step Toward Widespread Quantum Secure Cryptography Through the Cloud

https://www.businesswire.com/news/home/20210609005154/en/Qrypt-Makes-First-Step-Toward-Widespread-Quantum-Secure-Cryptography-Through-the-Cloud

Qrypt, a producer of cryptographic quantum security solutions enabled by Quantum Entropy-as-a-Service (EaaS), is emerging from stealth and announcing today the launch of its Cloud Entropy Portal. This world’s first virtual EaaS solution provides fast access to high-quality Quantum Random Number Generators (QRNG) hardware.

The Cloud Entropy Portal democratizes the availability of quantum safe random numbers for any application, especially cryptographic key generation. Perfect randomness is essential for both classical and Post-Quantum Cryptography (PQC), which requires vastly larger key sizes – up to full one-time pad systems. In addition to the Cloud Entropy Portal, Qrypt will soon unveil additional quantum data-at-rest and data-in-motion SDKs for any business, organization, or government agency to integrate quantum security into their applications.

“My time in the CIA led me to believe privacy is a fundamental right, and everyone should have access to CIA-level security – which is why I started Qrypt,” said Kevin Chalker, Qrypt’s CEO and founder. “Rapid advances in quantum computing make our current data security obsolete and put us on the verge of a once-in-a-generation transformation of cybersecurity.”

Qrypt’s technology massively scales quantum secure encryption, avoiding the high infrastructure investment in proprietary Quantum Key Distribution (QKD) appliances. Instead of satellite installations

and dedicated fiber optic cabling, Qrypt has digitized the simultaneous key generation of QKD through an authenticated network of QRNGs in the cloud. Useful for both classical cryptography and PQC, this approach eliminates the problem of replicated or predictable keys found across modern IP networks. Qrypt will empower any business or organization to enjoy the same national-security level of encryption the White House utilized for the "Red Phone" – the Washington-Moscow Direct Communications Link for quantum-secure communications with the Kremlin.

For businesses requiring the highest level of security and privacy for their customers and applications, Qrypt's technology will be the brass ring. Combining EaaS and PQC encryption nullifies a breach's impact since stolen data can never be decrypted – even by quantum computers. Implementing Qrypt's SDK neutralizes the "harvest now, decrypt later" tactics performed across global networks for decades. DevOps teams at any enterprise, financial institution, healthcare organization or government agency will have the essential tools and raw materials to meet the security challenges of the quantum age, which is an "extinction event" for the current public key infrastructure.

"Quantum computers are an existential threat to data security because they can calculate cryptographic keys in seconds, an impossible feat for the combined power of all the current supercomputers in existence," said Denis Mandich, Qrypt CTO and co-founder. "Cybercriminals and hostile state actors will leverage these quantum machines to exploit data on an industrial scale, compromising our privacy, national security and ultimately our economic future."

In founding Qrypt, Kevin and Denis hand-selected a talented team of seasoned leaders in engineering, physics, and cryptography to help build Qrypt's patented solutions suite. Key amongst them is Qrypt's chief cryptographer Yevgeniy Dodis, Ph.D., an IACR fellow and global leader in cryptography research focused on random number generation, protocol composition and information-theoretic cryptography. Combining Kevin's vision, Denis' experience, Dr. Yevgeniy's research, and the team's deep security expertise, Qrypt laid the groundwork for a revolutionary new approach to data security for the quantum computing age.

The company spent years on quantum cryptography research and development before launching a solution. Strategic partnerships with leading domestic, national and international labs provided exclusive access to quantum entropy sources and advanced technologies – many of which did not exist a decade ago. All of Qrypt's research is published and validated in peer-reviewed journals by professional experts in their field – there are no black boxes or unproven science. Qrypt also holds an international issued patent portfolio in the US, Europe, Japan and Korea, with eight patents and 100+ claims.

34 Tight finite-key analysis for quantum key distribution without monitoring signal disturbance

by npj quantum information

https://www.nature.com/articles/s41534-021-00428-9

Unlike traditional communication, quantum key distribution (QKD) can reach unconditional security and thus attracts intensive studies. Among all existing QKD protocols, round-robin-differential-phase-shift (RRDPS) protocol can be running without monitoring signal disturbance, which significantly simplifies its flow and improves its tolerance of error rate. Although several security proofs of RRDPS have been given, a tight finite-key analysis with a practical phase-randomized source is still missing. In the paper, authors propose an improved security proof of RRDPS against the most general coherent attack based on the entropic

uncertainty relation. What's more, with the help of Azuma's inequality, their proof can tackle finite-key effects primely. The proposed finite-key analysis keeps the advantages of phase randomization source and indicates experimentally acceptable numbers of pulses are sufficient to approach the asymptotical bound closely. The results shed light on practical QKD without monitoring signal disturbance.

08 Jun 2021

35 What Makes Quantum Computing So Hard to Explain?

by Scott Aaronson

https://www.quantamagazine.org/why-is-quantum-computing-so-hard-to-explain-20210608/

Quantum computers, you might have heard, are magical uber-machines that will soon cure cancer and global warming by trying all possible answers in different parallel universes. For 15 years, on my blog and elsewhere, I've railed against this cartoonish vision, trying to explain what I see as the subtler but ironically even more fascinating truth. I approach this as a public service and almost my moral duty as a quantum computing researcher. Alas, the work feels Sisyphean: The cringeworthy hype about quantum computers has only increased over the years, as corporations and governments have invested billions, and as the technology has progressed to programmable 50-qubit devices that (on certain contrived benchmarks) really can give the world's biggest supercomputers a run for their money. And just as in cryptocurrency, machine learning and other trendy fields, with money have come hucksters.

In reflective moments, though, I get it. The reality is that even if you removed all the bad incentives and the greed, quantum computing would still be hard to explain briefly and honestly without math. As the quantum computing pioneer Richard Feynman once said about the quantum electrodynamics work that won him the Nobel Prize, if it were possible to describe it in a few sentences, it wouldn't have been worth a Nobel Prize.

Not that that's stopped people from trying. Ever since Peter Shor discovered in 1994 that a quantum computer could break most of the encryption that protects transactions on the internet, excitement about the technology has been driven by more than just intellectual curiosity. Indeed, developments in the field typically get covered as business or technology stories rather than as science ones.

That would be fine if a business or technology reporter could truthfully tell readers, "Look, there's all this deep quantum stuff under the hood, but all you need to understand is the bottom line: Physicists are on the verge of building faster computers that will revolutionize everything."

The trouble is that quantum computers will not revolutionize everything.

Yes, they might someday solve a few specific problems in minutes that (we think) would take longer than the age of the universe on classical computers. But there are many other important problems for which most experts think quantum computers will help only modestly, if at all. Also, while Google and others recently made credible claims that they had achieved contrived quantum speedups, this was only for specific, esoteric benchmarks (ones that I helped develop). A quantum computer that's big and reliable enough to outperform classical computers at practical applications like breaking cryptographic codes and simulating chemistry is likely still a long way off.

But how could a programmable computer be faster for only some problems? Do we know which ones? And what does a "big and reliable" quantum computer even mean in this context? To answer these questions

we have to get into the deep stuff.

Let's start with quantum mechanics. (What could be deeper?) The concept of superposition is infamously hard to render in everyday words. So, not surprisingly, many writers opt for an easy way out: They say that superposition means "both at once," so that a quantum bit, or qubit, is just a bit that can be "both 0 and 1 at the same time," while a classical bit can be only one or the other. They go on to say that a quantum computer would achieve its speed by using qubits to try all possible solutions in superposition – that is, at the same time, or in parallel.

This is what I've come to think of as the fundamental misstep of quantum computing popularization, the one that leads to all the rest. From here it's just a short hop to quantum computers quickly solving something like the traveling salesperson problem by trying all possible answers at once – something almost all experts believe they won't be able to do.

The thing is, for a computer to be useful, at some point you need to look at it and read an output. But if you look at an equal superposition of all possible answers, the rules of quantum mechanics say you'll just see and read a random answer. And if that's all you wanted, you could've picked one yourself.

What superposition really means is "complex linear combination." Here, we mean "complex" not in the sense of "complicated" but in the sense of a real plus an imaginary number, while "linear combination" means we add together different multiples of states. So a qubit is a bit that has a complex number called an amplitude attached to the possibility that it's 0, and a different amplitude attached to the possibility that it's 1. These amplitudes are closely related to probabilities, in that the further some outcome's amplitude is from zero, the larger the chance of seeing that outcome; more precisely, the probability equals the distance squared.

But amplitudes are not probabilities. They follow different rules. For example, if some contributions to an amplitude are positive and others are negative, then the contributions can interfere destructively and cancel each other out, so that the amplitude is zero and the corresponding outcome is never observed; likewise, they can interfere constructively and increase the likelihood of a given outcome. The goal in devising an algorithm for a quantum computer is to choreograph a pattern of constructive and destructive interference so that for each wrong answer the contributions to its amplitude cancel each other out, whereas for the right answer the contributions reinforce each other. If, and only if, you can arrange that, you'll see the right answer with a large probability when you look. The tricky part is to do this without knowing the answer in advance, and faster than you could do it with a classical computer.

Twenty-seven years ago, Shor showed how to do all this for the problem of factoring integers, which breaks the widely used cryptographic codes underlying much of online commerce. We now know how to do it for some other problems, too, but only by exploiting the special mathematical structures in those problems. It's not just a matter of trying all possible answers at once.

Compounding the difficulty is that, if you want to talk honestly about quantum computing, then you also need the conceptual vocabulary of theoretical computer science. I'm often asked how many times faster a quantum computer will be than today's computers. A million times? A billion?

This question misses the point of quantum computers, which is to achieve better "scaling behavior," or running time as a function of n, the number of bits of input data. This could mean taking a problem where the best classical algorithm needs a number of steps that grows exponentially with n, and solving it using a number of steps that grows only as n^2. In such cases, for small n, solving the problem with a quantum computer will actually be slower and more expensive than solving it classically. It's only as n grows that the quantum speedup first appears and then eventually comes to dominate.

But how can we know that there's no classical shortcut – a conventional algorithm that would have similar scaling behavior to the quantum algorithm's? Though typically ignored in popular accounts, this question is central to quantum algorithms research, where often the difficulty is not so much proving that a quantum computer can do something quickly, but convincingly arguing that a classical computer can't. Alas, it turns out to be staggeringly hard to prove that problems are hard, as illustrated by the famous P versus NP problem (which asks, roughly, whether every problem with quickly checkable solutions can also be quickly solved). This is not just an academic issue, a matter of dotting i's: Over the past few decades, conjectured quantum speedups have repeatedly gone away when classical algorithms were found with similar performance.

Note that, after explaining all this, I still haven't said a word about the practical difficulty of building quantum computers. The problem, in a word, is decoherence, which means unwanted interaction between a quantum computer and its environment – nearby electric fields, warm objects, and other things that can record information about the qubits. This can result in premature "measurement" of the qubits, which collapses them down to classical bits that are either definitely 0 or definitely 1. The only known solution to this problem is quantum error correction: a scheme, proposed in the mid-1990s, that cleverly encodes each qubit of the quantum computation into the collective state of dozens or even thousands of physical qubits. But researchers are only now starting to make such error correction work in the real world, and actually putting it to use will take much longer. When you read about the latest experiment with 50 or 60 physical qubits, it's important to understand that the qubits aren't error-corrected. Until they are, we don't expect to be able to scale beyond a few hundred qubits.

Once someone understands these concepts, I'd say they're ready to start reading – or possibly even writing – an article on the latest claimed advance in quantum computing. They'll know which questions to ask in the constant struggle to distinguish reality from hype. Understanding this stuff really is possible – after all, it isn't rocket science; it's just quantum computing!

36 Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics

by npj Quantum Information

https://www.nature.com/articles/s41534-021-00421-2

The future envisaged global-scale quantum-communication network will comprise various nodes interconnected via optical fibers or free-space channels, depending on the link distance. The free-space segment of such a network should guarantee certain key requirements, such as daytime operation and the compatibility with the complementary telecom-based fiber infrastructure. In addition, space-to-ground links will require the capability of designing light and compact quantum devices to be placed in orbit. For these reasons, investigating available solutions matching all the above requirements is still necessary. In the article authors present a full prototype for daylight quantum key distribution at 1550 nm exploiting an integrated silicon-photonics chip as state encoder. They tested their prototype in the urban area of Padua (Italy) over a 145 m-long free-space link, obtaining a quantum bit error rate around 0.5% and an averaged secret key rate of 30 kbps during a whole sunny day (from 11:00 to 20:00). The developed chip represents a cost-effective solution for portable free-space transmitters and a promising resource to design quantum optical payloads for future satellite missions.

37 Early endeavors on the path to reliable quantum machine learning

by ETH Zurich

https://www.sciencedaily.com/releases/2021/06/210608083951.htm

Intelligent machine learning methods can recognise patterns or objects and automatically pick them out of data sets. For example, they could pick out those pictures from a photo database that show non-toxic mushrooms. Particularly with very large and complex data sets, machine learning can deliver valuable results that humans would not be able to find out, or only with much more time. However, for certain computational tasks, even the fastest computers available today reach their limits. This is where the great promise of quantum computers comes into play: that one day they will also perform super-fast calculations that classical computers cannot solve in a useful period of time.

The reason for this "quantum supremacy" lies in physics: quantum computers calculate and process information by exploiting certain states and interactions that occur within atoms or molecules or between elementary particles.

The fact that quantum states can superpose and entangle creates a basis that allows quantum computers the access to a fundamentally richer set of processing logic. For instance, unlike classical computers, quantum computers do not calculate with binary codes or bits, which process information only as 0 or 1, but with quantum bits or qubits, which correspond to the quantum states of particles. The crucial difference is that qubits can realise not only one state – 0 or 1 – per computational step, but also a state in which both superpose. These more general manners of information processing in turn allow for a drastic computational speed-up in certain problems.

Translating classical wisdom into the quantum realm

These speed advantages of quantum computing are also an opportunity for machine learning applications – after all, quantum computers could compute the huge amounts of data that machine learning methods need to improve the accuracy of their results much faster than classical computers.

However, to really exploit the potential of quantum computing, one has to adapt the classical machine learning methods to the peculiarities of quantum computers. For example, the algorithms, i.e. the mathematical calculation rules that describe how a classical computer solves a certain problem, must be formulated differently for quantum computers. Developing well-functioning "quantum algorithms" for machine learning is not entirely trivial, because there are still a few hurdles to overcome along the way.

On the one hand, this is due to the quantum hardware. At ETH Zurich, researchers currently have quantum computers that work with up to 17 qubits. However, if quantum computers are to realise their full potential one day, they might need thousands to hundreds of thousands of qubits.

Quantum noise and the inevitability of errors

One challenge that quantum computers face concerns their vulnerability to error. Today's quantum computers operate with a very high level of "noise," as errors or disturbances are known in technical jargon. For the American Physical Society, this noise is " the major obstacle to scaling up quantum computers." No comprehensive solution exists for both correcting and mitigating errors. No way has yet been found

to produce error-free quantum hardware, and quantum computers with 50 to 100 qubits are too small to implement correction software or algorithms.

To a certain extent, one has to live with the fact that errors in quantum computing are in principle unavoidable, because the quantum states on which the concrete computational steps are based can only be distinguished and quantified with probabilities. What can be achieved, on the other hand, are procedures that limit the extent of noise and perturbations to such an extent that the calculations nevertheless deliver reliable results. Computer scientists refer to a reliably functioning calculation method as "robust" and in this context also speak of the necessary "error tolerance."

This is exactly what the research group led by Ce Zhang, ETH computer science professor and member of the ETH AI Center, has has recently explored, somehow "accidentally" during an endeavor to reason about the robustness of classical distributions for the purpose of building better machine learning systems and platforms. Together with Professor Nana Liu from Shanghai Jiao Tong University and with Professor Bo Li from the University of Illinois at Urbana, they have developed a new approach. This allows them to prove the robustness conditions of certain quantum-based machine learning models, for which the quantum computation is guaranteed to be reliable and the result to be correct. The researchers have published their approach, which is one of the first of its kind, in the scientific journal npj Quantum Information.

Protection against errors and hackers

"When we realised that quantum algorithms, like classical algorithms, are prone to errors and perturbations, we asked ourselves how we can estimate these sources of errors and perturbations for certain machine learning tasks, and how we can guarantee the robustness and reliability of the chosen method," says Zhikuan Zhao, a postdoc in Ce Zhang's group. "If we know this, we can trust the computational results, even if they are noisy."

The researchers investigated this question using quantum classification algorithms as an example – after all, errors in classification tasks are tricky because they can affect the real world, for example if poisonous mushrooms were classified as non-toxic. Perhaps most importantly, using the theory of quantum hypothesis testing – inspired by other researchers' recent work in applying hypothesis testing in the classical setting – which allows quantum states to be distinguished, the ETH researchers determined a threshold above which the assignments of the quantum classification algorithm are guaranteed to be correct and its predictions robust.

With their robustness method, the researchers can even verify whether the classification of an erroneous, noisy input yields the same result as a clean, noiseless input. From their findings, the researchers have also developed a protection scheme that can be used to specify the error tolerance of a computation, regardless of whether an error has a natural cause or is the result of manipulation from a hacking attack. Their robustness concept works for both hacking attacks and natural errors.

"The method can also be applied to a broader class of quantum algorithms," says Maurice Weber, a doctoral student with Ce Zhang and the first author of the publication. Since the impact of error in quantum computing increases as the system size rises, he and Zhao are now conducting research on this problem. "We are optimistic that our robustness conditions will prove useful, for example, in conjunction with quantum algorithms designed to better understand the electronic structure of molecules."

07 Jun 2021

38 Q-Day Is Coming Sooner Than We Think

by Arthur Herman

https://www.forbes.com/sites/arthurherman/2021/06/07/q-day-is-coming-sooner-than-we-think/?utm_medium=email&_hsmi=137284072&_hsenc=p2ANqtz-9wvPTak1c6oNIzz8x56UeCWyP68m_qb_yD9l-y2m4r5tJwiu0PTZBWqso1t1ynYYHx6g0OypaeqJS-fmLlw7ORLzLX6g&utm_content=137284072&utm_source=hs_email&sh=285d44863f5d

"Q-Day" is the term some experts use to describe when large-scale quantum computers are able to factorize the large prime numbers that underlie our public encryption systems, such as the ones that are supposed to protect our bank accounts, financial markets, and most vital infrastructure. That's a feat that's all but impossible for even the fastest supercomputers but which the unique features of quantum computers, using the physics of superpositioning and entanglement, will be able to deliver.

There's a growing consensus that this quantum threat is real; there's no agreement how long it will take before a quantum computer has the 4000 or so stable qubits it will need to meet the requirements of Shor's algorithm for cracking those encryption systems.

For example, it would take a classical computer 300 trillion years to crack an RSA-2048 bit encryption key. A quantum computer can do the same job in just ten seconds with 4099 stable qubits – but getting to that number is the main problem quantum computer engineers face since the stability or coherence of qubits lasts only for microseconds. Today's most entangled computer, Google's Bristlecone, has just 72 stable qubits.

Nonetheless, I have been arguing for the past four years, including in this column, that Q-Day is likely to come sooner than even quantum scientists can predict, and that the time to get ready to protect our vulnerable data and networks is now. Others prefer to procrastinate, citing other experts who say such a threat is at least a decade or more away. The fact that the National Institute of Standards and Technology won't have its quantum-resistant algorithm standards ready until 2024, and expects the rollout to space out for another five to fifteen years, has helped to encourage complacency disguised as confidence.

But new developments in quantum science suggest that this complacency is misplaced. If the large-scale quantum computer is the ultimate thermonuclear device in cyberwarfare, the dirty bomb is the quantum annealer – and it's probably going to be here sooner than even experts thought.

So-called quantum annealers like the one Canada-based D-Wave Systems, Inc. uses, are able to calculate the lowest energy level between the qubits' different states of entanglement, which equals the optimal solution. These machines have proven their worth in solving optimization problems that usually stump classical computers.

Not surprisingly, scientists have been quietly finding ways to turn factorization – the decryption process that leads to Q-Day – into an optimization problem instead of relying Shor's algorithm, the paradigm for discussing quantum decryption since the 1990's. In 2019 scientific papers emerged that showed how to do this, including factorizing integers using "noisy" qubits, i.e. swarms of quantum bits that aren't perfectly entangled the way a large-scale computer requires.

One was authored by Chinese scientists who found a way to factor a large number using only 89 noisy qubits. They then showed it's possible to factorize a RSA-768 encryption number – the current factorization record using classical computers – with 147,454 noisy qubits. That's a tiny fraction of the millions of qubits a large quantum computer would need to reach the 4000 stable qubit threshold, and within reach of the architecture of an annealer like D-Wave Systems.

That same year a pair of researchers from Google and the Royal Institute of Technology at Stockholm

published a paper showing how to crack 2028-bit RSA integers in 8 hours using 20 million noisy qubits. Given the fact that in 2012 scientists speculated that it would take 1 billion qubits to perform this feat, it won't be long before researchers show they can get there with a lot fewer than 20 million qubits.

Sure enough, in 2020 three Chinese researchers found a way to use the D-Wave quantum computer to factorize large integers, that completely bypasses Shor's algorithm. "Thus," they concluded, "post-quantum cryptography should consider further the potential of the D-Wave quantum computer for deciphering the RSA cryptosystem in future."

In effect, these researchers found a way to turn decryption using quantum technology into a straightforward process on a timeline much shorter than ten years: perhaps four to five years is more likely.

This was what Chinese scientists are openly publishing. We don't know what's happening behind the scenes, but we can bet if there's a short cut to achieve what a large-scale quantum computer can do using annealing technology, their military and intelligence services will want to find out.

All this changes the timetable for Q-Day significantly, and our strategic calculations. Not only is quantum-based decryption coming our way sooner, but thanks to annealing that code-breaking feature will be more accessible to other machines than the hugely expensive large-scale computers Google, Microsoft, and others are working on – which puts the threat within reach of small-state or even non-state actors.

That's why the dirty bomb analogy is so apt. Why gamble with the quantum future? Annealing technology makes getting quantum ready more important, and getting started now, more imperative than ever.

39 Council for New Industry Creation through Quantum Technology Being Formed in Japan

https://quantumcomputingreport.com/council-for-new-industry-creation-through-quantum-technology-being-formed-in-japan/

Eleven Japanese companies known as the Founders Association met at the end of May and are planning to launch this summer a Council for New Industry Creation through Quantum Technology. The Council will promote the application of quantum technologies to the creation of new industries over the medium to long term in Japan. Personnel from industry, academia and government will work together to investigate general trends in quantum technology, materials, and devices, investigate and make recommendations on application of the technology and the required industrial structure, systems and rules.

The companies participating in the Founders Association for this council include the following:

- Dai-ichi Life Holdings, Inc.
- Fujitsu Limited
- Hitachi, Ltd. JSR Corporation
- JSR Corporation
- Mitsubishi Chemical Holdings Corporation
- Mizuho Financial Group, Inc.

- NEC Corporation
- Nippon Telegraph and Telephone Corporation
- Tokio Marine Holdings, Inc.
- Toshiba Corporation
- Toyota Motor Corporation

40 Ransomware Struck Another Pipeline Firm – and 70GB of Data Leaked

by andy greenberg

https://www.wired.com/story/linestar-pipeline-ransomware-leak/

WHEN RANSOMWARE HACKERS hit Colonial Pipeline last month and shut off the distribution of gas along much of the East Coast of the United States, the world woke up to the danger of digital disruption of the petrochemical pipeline industry. Now it appears another pipeline-focused business was also hit by a ransomware crew around the same time, but kept its breach quiet – even as 70 gigabytes of its internal files were stolen and dumped onto the dark web.

A group identifying itself as Xing Team last month posted to its dark web site a collection of files stolen from LineStar Integrity Services, a Houston-based company that sells auditing, compliance, maintenance, and technology services to pipeline customers. The data, first spotted online by the WikiLeaks-style transparency group Distributed Denial of Secrets, or DDoSecrets, includes 73,500 emails, accounting files, contracts, and other business documents, around 19 GB of software code and data, and 10 GB of human resources files that includes scans of employee driver's licenses and Social Security cards. And while the breach doesn't appear to have caused any disruption to infrastructure like the Colonial Pipeline incident, security researchers warn the spilled data could provide hackers a roadmap to more pipeline targeting.

DDoSecrets, which makes a practice of trawling data leaked by ransomware groups as part of its mission to expose data it deems worthy of public scrutiny, published 37 gigabytes of the company's data to its leak site on Monday. The group says it was careful to redact potentially sensitive software data and code – which DDoSecrets says could enable follow-on hackers to find or exploit vulnerabilities in pipeline software – as well as the leaked human resources material, in an effort to leave out LineStar employees' sensitive, personally identifiable information.

But the unredacted files, which WIRED has reviewed, remain online. And they may include information that could enable follow-on targeting of other pipelines, argues Joe Slowik, a threat intelligence researcher for security firm Gigamon who has focused on critical infrastructure security for years as the former head of incident response at Los Alamos National Labs. While Slowik notes that it's still not clear what sensitive information might be included in the leak's 70 GB, he worries that it could include information about the software architecture or physical equipment used by LineStar's customers, given that LineStar provides information technology and industrial control system software to pipeline customers.

"You can use that to fill in lots of targeting data, depending on what's in there," says Slowik. "It's very concerning, given the potential that it's not just about people's driver's license information or other HR

related items, but potentially data that relates to the operation of these networks and their more critical functionality."

Xing Team is a relatively new entrant to the ransomware ecosystem. But while the group writes its name with a Chinese character on its dark web site – and comes from the Mandarin word for "star" – there's little reason to believe the group is Chinese based on that name alone, says Brett Callow, a ransomware-focused researcher with antivirus firm Emsisoft. Callow says he's seen Xing Team use the rebranded version of Mount Locker malware to encrypt victims' files, as well as threaten to leak the unencrypted data as a way to extort targets into paying. In the case of LineStar, Xing Team appears to have followed through on that threat.

That leak could in turn serve as a stepping stone for other ransomware hackers, who frequently comb dark web data dumps for information that can be used to impersonate companies and target their customers. "If you were to steal data from a pipeline company, that could possibly enable you to construct a fairly conventional spearphishing email to another pipeline company," says Callow. "We absolutely know that groups do that."

LineStar did not respond to multiple requests for comment prior to publication, but sent an emailed statement several hours after this story went live. "LineStar is a small, private company and we were the victim of a ransomware attack in late April that targeted corporate data. There was no impact to either internal or customer operations," said LineStar CFO Chris Boston in the statement. "Immediately following the attack, we notified our employees of a potential breach involving employee personal information, engaged third-party IT experts and notified the FBI. We have been taking every reasonable measure to protect our employees while responding to an internal data breach and subsequent theft." Boston further claimed that "comparisons made" in this story were "completely inaccurate and provably untrue," but did not provide any specific objections.

DDoSecrets' practice of republishing the leaked data of ransomware victims – even in a redacted form – has been criticized for amplifying ransomware groups' coercive techniques. But the group's cofounder Emma Best, who uses the pronoun "they," argues that doing so for the LineStar leak in particular helps to shine a spotlight on an industry with a long record of environmental scandals. The Colonial Pipeline itself leaked 1.2 million gallons of gasoline into a nature preserve in North Carolina less than a year prior to being targeted by ransomware, Best points out. "To torture a metaphor, fuel is the fuel of our economy, but it's also a poison when they frequently leak or the pipeline's construction, operation, or maintenance infringe on communities, typically already marginalized ones," Best told WIRED in a text interview.

Best notes that even the shutdown of the pipeline following Colonial's ransomware incident in May, which triggered gas shortages across the East Coast, wasn't primarily due to safety concerns, but business and billing issues. "This isn't an industry that has the public interest at heart," Best writes. They didn't confirm if they had found any evidence of wrongdoing in the leaked LineStar files, but argue that it's noteworthy either way. "With some industries, you have to stop and study them regardless of individual wrongdoing because the industry itself is either so inherently harmful or fraught with danger that to not study it would be reckless."

The breach of a second pipeline firm by ransomware operators after Colonial's shutdown may seem to signal a trend of cybercriminal hackers specifically targeting critical infrastructure. But Emsisoft's Brett Callow points out that ransomware groups like Xing Team are targeting companies mostly indiscriminately, casting a wide net as they seek to maximize their ransom payments.

"There has been a lot of talk about critical infrastructure being targeted in this war-like situation, but

that is really bullshit," Callow says. "They are just going after everybody. It's a feeding frenzy."

That hacking epidemic, however, now extends to the industrial backbone of the American economy. And with the breach of a company that serves as a hub of one such industry, the stakes are only getting higher.

04 Jun 2021

41 Messages scrambled by black holes stand their ground against quantum computers

by Jacob Marks

https://physicsworld.com/a/messages-scrambled-by-black-holes-stand-their-ground-against-quantum-computers/

Black holes are nature's fastest data-scramblers, and new research suggests that secrets thrown into them may be more secure than previously thought. In a paper published in Physical Review Letters, researchers at Los Alamos National Laboratory (LANL) in the US show that once a message has been scrambled by a black hole or another system with similar properties, not even a quantum computer can put it back together.

Scramblers are quantum systems that take local information and spread it across the entire system, generating quantum entanglement between distant regions. They crop up in various contexts in physics. While black holes are perhaps the most famous example, scramblers also exist in simple systems such as spin chains – 1D arrangements of quantum particles with coupling between nearest neighbours – and in "strange" metals, in which resistivity depends atypically on temperature.

Although the scrambling process is deterministic – a fixed input yields a fixed output – scrambling systems can give rise to tremendously complex behaviour, distributing information in seemingly random fashion. This emergence of apparent randomness is known as quantum chaos, in analogy with classical chaos theory, where similarly simple systems produce equally intricate dynamics.

A shred of hope for message recovery

Physicists working at the intersection of quantum mechanics and gravity are interested in scramblers in part thanks to the so-called black hole information paradox. The paradox revolves around the ultimate fate of information that falls past the event horizon and into a black hole: after a message is scrambled across the surface of a black hole, is its information trapped in the black hole forever, or does it somehow manage to escape? One school of thought holds that information does escape from black holes in the form of photons emitted via a process known as Hawking radiation. This theory received some corroboration in 2019, but the jury is still out.

In 2007, while investigating this paradox, physicists Patrick Hayden and John Preskill came up with a thought experiment. Assuming that black holes do encode information in Hawking radiation, they showed that when a message is sent into a black hole, its pieces can be rapidly recovered by capturing a few of the emitted photons – a process akin to recovering the slices of a shredded document from the heat given off by the shredder. However, while the black hole's scrambling behaviour makes such a recovery possible, the Hawking radiation alone doesn't tell you how to unscramble a scrambled message. Other approaches are needed to, in effect, reassemble the shredded document from its paper strips.

Scramblers beset by barren plateaus

Enter machine learning algorithms. These powerful pattern-identifying tools "learn" how to best approximate a physical system by comparing outputs of the real system to their own outputs (given the same inputs for both), tweaking their internal model, and then rinsing and repeating until reality and approximation align. The central quantity in this learning process is a mathematical quantity known as the cost function, which captures the degree of deviation between the model and the real system.

In classical machine-learning methods, the cost function is like a mountain range, replete with peaks and troughs that represent its higher and lower values. Minimizing the cost function – and learning a model for the system – is like finding a descending path and following it down to base camp. When the model is a quantum system modelled on a quantum computer, however, the cost function landscape isn't always so rich. In fact, the LANL researchers showed that when the algorithm is asked to model a scrambler, it suffers from the problem of "barren plateaus". "The cost function is essentially flat everywhere, with a needle-sized hole that is the base," says Zoe Holmes, a postdoctoral scholar at LANL and lead author on the paper.

This absence of features in the cost function renders quantum machine learning ineffective, because finding the "hole" from a random starting point within the landscape is almost impossible without a downward path to follow. "If you're learning using a cost function evaluated on a quantum computer, no matter how many training pairs you have, you won't be able to learn the scrambler," Holmes says, "at least without prior knowledge". This flaw rules out the possibility of reconstructing a message, which would entail inverting the scrambling process.

A hard lesson to learn

The LANL researchers conclude that even if the pieces of a scrambled message are known, putting them back together poses a problem that quantum computers cannot help us solve. "You could perhaps (ambitiously!) try to use the fundamental physics of the black hole to put a message together," says Holmes, cautioning that no such method is currently known, "but any learning method looks pretty doomed". Nature, it seems, is a pretty good confidant.

42 U.S. to give ransomware hacks similar priority as terrorism

by Christopher Bing

https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

The U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority as terrorism in the wake of the Colonial Pipeline hack and mounting damage caused by cyber criminals, a senior department official told Reuters.

Internal guidance sent on Thursday to U.S. attorney's offices across the country said information about ransomware investigations in the field should be centrally coordinated with a recently created task force in Washington.

"It's a specialized process to ensure we track all ransomware cases regardless of where it may be referred in this country, so you can make the connections between actors and work your way up to disrupt the whole chain," said John Carlin, principle associate deputy attorney general at the Justice Department.

Last month, a cyber criminal group that the U.S. authorities said operates from Russia, penetrated the pipeline operator on the U.S. East Coast, locking its systems and demanding a ransom. The hack caused a shutdown lasting several days, led to a spike in gas prices, panic buying and localized fuel shortages in the southeast.

Colonial Pipeline decided to pay the hackers who invaded their systems nearly $5 million to regain access, the company said.

The DOJ guidance specifically refers to Colonial as an example of the "growing threat that ransomware and digital extortion pose to the nation."

"To ensure we can make necessary connections across national and global cases and investigations, and to allow us to develop a comprehensive picture of the national and economic security threats we face, we must enhance and centralize our internal tracking," said the guidance seen by Reuters and previously unreported.

The Justice Department's decision to push ransomware into this special process illustrates how the issue is being prioritized, U.S. officials said.

"We've used this model around terrorism before but never with ransomware," said Carlin. The process has typically been reserved for a short list of topics, including national security cases, legal experts said.

In practice, it means that investigators in U.S. attorney's offices handling ransomware attacks will be expected to share both updated case details and active technical information with leaders in Washington.

The guidance also asks the offices to look at and include other investigations focused on the larger cybercrime ecosystem.

According to the guidance, the list of investigations that now require central notification include cases involving: counter anti-virus services, illicit online forums or marketplaces, cryptocurrency exchanges, bulletproof hosting services, botnets and online money laundering services.

Bulletproof hosting services refer to opaque internet infrastructure registration services which help cyber criminals to anonymously conduct intrusions.

A botnet is a group of compromised internet-connected devices that can be manipulated to cause digital havoc. Hackers build, buy and rent out botnets in order to conduct cyber crimes ranging from advertising fraud to large cyberattacks.

"We really want to make sure prosecutors and criminal investigators report and are tracking ... cryptocurrency exchanges, illicit online forums or marketplaces where people are selling hacking tools, network access credentials – going after the botnets that serve multiple purposes," said Carlin.

Mark Califano, a former U.S. attorney and cybercrime expert, said the "heightened reporting could allow DOJ to more effectively deploy resources" and to "identify common exploits" used by cybercriminals.

43 Quantum Nation Switzerland – Good, but there's something missing

by Christoph Ebell

https://www.swissquantumhub.com/quantum-nation-switzerland-good-but-theres-something-missing/

SwissICT is the largest Swiss association for the ICT industry. Its recently established Policy Commission sent a letter to the Federal Council expressing the association's concern about the possible exclusion of Switzerland from the Horizon Europe research programme in the fields of quantum and space research. The President of the Swiss Confederation, Guy Parmelin, sent a reply, and we have a first positive result. Here is a brief appreciation, context, and commentary. And a billion-frac proposal for a Swiss Quantum fund.

First of all, it is important and good to know that the Federal Council is aiming for full accession to "Horizon Europe" (HEU) – even from today's perspective. This is also confirmed by the President of the Confederation: 6 billion have been decided for HEU and the ITER, Euratom, and Digital Europe programmes. So, there is no lack of will on the part of our executive. At the same time, however, the President warned that the EU Commission has already signalled those corresponding talks will be made dependent on "progress" in the Framework Agreement.

This is now history: Switzerland pulled out of the negotiations. As a result, the matter just became more urgent.

According to the letter from the President of the Swiss Confederation, the responsible department, i.e., the State Secretariat for Education, Research and Innovation (SERI), share swissICT's concerns regarding the exclusion from the programme components mentioned. This is especially true in view of the fact that Switzerland is significantly involved in the development of the technologies in question or plays a leading role. It is now SERI's task to implement "Plan B" – and I'm informed that they have one ready in anticipation of this outcome.

In the meantime, Switzerland's efforts seem to have had an effect. In the new draft of the programme, Switzerland was apparently again involved in quantum research. Whether or not this will still be the case now after the end of the framework agreement negotiations remains to be seen. Adjustments will have to be made. Nevertheless, whatever our science diplomats have done: Good job!

What can we learn? I'm focusing on quantum technology here, because it's more the field of swissICT – but that doesn't mean space is any less important, in fact the two are linked. The University of Geneva, the Swiss Quantum Hub, the Paul Scherrer Institute, the ETH, IBM Research in Zurich, CSEM and several other large and small players are driving forces in our country. A white paper published last year by the Swiss Science Council (SSC) clearly shows that the quantum research strategy in Switzerland, with the national research focus QSIT and preceding NCCRs in this area, has borne fruit and Swiss groups occupy leading positions internationally. Companies such as Terra Quantum, ID Quantique, startups like Qnami, just to name a few, point to the economic growth potential. The reputation of Swiss precision technology is legendary – and a key resource for quantum systems.

Switzerland occupies a top international position in quantum research and the Swiss science system does good, even excellent work. The EU wants technological sovereignty – independence from the USA and China in strategic technologies – both economically and in terms of security policy.

Clearly, Switzerland is perfectly positioned for quantum growth. So much everyone seems to agree on, and it is also clear to our partners in the EU Commission.

This leads us to the second conclusion: Switzerland is a highly attractive partner in quantum technology and this circumstance has probably also helped our "re-entry" at least in the current draft of the "Horizon Europe" work programme, and it will be key for the arrangements post-framework agreement.

So, is everything OK?

No.

The SSC report also demonstrates that. What is missing in Switzerland (and it is an old and recurring tale in our innovation system) is well-diversified venture capital, including for early funding rounds. If we want to see quantum innovation and growth in Switzerland, we cannot afford to sit on our hands.

I therefore propose two types of action:

(i) Establish quantum technology experimentation stations in Switzerland where start-ups, established companies, users, and researchers can build and test realistic "sandbox" scenarios and experimental ecosystems. We already have the technology for this, and the Quantum Hub model is inspiring.

(ii) Establish a CHF 1 billion private quantum technology investment fund for Swiss start-ups and scale-ups, with a special focus (33%?) on early-stage funding with a high-risk profile.

The federal government can help here, perhaps not with direct funds, but possibly by absorbing part of the risk or other structural accompanying measures as part of the Covid recovery strategy. However, it is primarily the financial industry and investors who are called upon – money is available and Swiss quantum technology is an enormous investment opportunity.

My contribution can be the coordination of a fund consortium. Write to me or the swissICT office with ideas and pledges. Since this opinion piece first appeared I have had some very interesting conversations, including with Julien Levallois at the Swiss Quantum Hub in Geneva and several enterprises. We plan get together and see how we can move this forward, knowing full well that this isn't the first attempt. We also know that the opportunities for the Quantum Nation Switzerland are too great to give up.

03 Jun 2021

44 Scientists found a new and promising qubit at a place where there is nothing

by Institute of Science and Technology Austria

https://www.sciencedaily.com/releases/2021/06/210603111940.htm

Quantum computers with their promises of creating new materials and solving intractable mathematical problems are a dream of many physicists. Now, they are slowly approaching viable realizations in many laboratories all over the world. But there are still enormous challenges to master. A central one is the construction of stable qubit that can be networked together.

In a study published in Nature Materials and led by Daniel Jirovec from the Katsaros group at IST Austria in close collaboration with researchers from the L-NESS Inter-university Centre in Como, Italy, scientists now have created a new and promising candidate system for reliable qubits.

Spinning Absence

The researchers created the qubit using the spin of so-called holes. Each hole is just the absence of an electron in a solid material. Amazingly, a missing negatively charged particle can physically be treated as

if it were a positively charged particle. It can even move around in the solid when a neighboring electron fills the hole. Thus, effectively the hole described as positively charged particle is moving forward.

These holes even carry the quantum-mechanical property of spin and can interact if they come close to each other. "Our colleagues at L-NESS layered several different mixtures of silicon and germanium just a few nanometers thick on top of each other. That allows us to confine the holes to the germanium-rich layer in the middle," Jirovec explains. "On top, we added tiny electrical wires – so-called gates – to control the movement of holes by applying voltage to them. The electrically positively charged holes react to the voltage and can be extremely precisely moved around within their layer."

Using this nano-scale control, the scientists moved two holes close to each other to create a qubit out of their interacting spins. But to make this work, they needed to apply a magnetic field to the whole setup. Here, their innovative approach comes into play.

Linking Qubits

In their setup, Jirovec and his colleagues cannot only move holes around but also alter their properties. By engineering different hole properties, they created the qubit out of the two interacting hole spins using less than ten millitesla of magnetic field strength. This is a weak magnetic field compared to other similar qubit setups, which employ at least ten times stronger fields.

But why is that relevant? "By using our layered germanium setup we can reduce the required magnetic field strength and therefore allow the combination of our qubit with superconductors, usually inhibited by strong magnetic fields," Jirovec says. Superconductors – materials without any electrical resistance – support the linking of several qubits due to their quantum-mechanical nature. This could enable scientists to build new kinds of quantum computers combining semiconductors and superconductors.

In addition to the new technical possibilities, these hole spin qubits look promising because of their processing speed. With up to one hundred million operations per second as well as their long lifetime of up to 150 microseconds they seem particularly viable for quantum computing. Usually, there is a tradeoff between these properties, but this new design brings both advantages together.

45 Reimagining enterprise cryptography: How to regain control in a fragmented environment

by Yehuda Lindell

https://www.helpnetsecurity.com/2021/06/03/reimagining-cryptography-for-the-enterprise/

Cryptography has been on a significant journey over the past two decades. Its role in securing the digital world of 20 years ago was very different to its role in the modern enterprise. Today, it is understood that attackers are everywhere, and we cannot rely on a strong perimeter to keep them out. This requires organizations to deploy zero-trust solutions, where security is preserved even when attackers manage to get into the network.

The challenge is compounded by new ways of working such as BYOD, remote working, and the spreading of IT infrastructure across data centers and clouds, all of which now needs to be managed remotely. In this modern environment, cryptography is needed everywhere. Unfortunately, the need to deploy cryptographic solutions enterprise-wide, at the pace needed by business, comes with many challenges.

At the heart of the matter is the fact that the current cryptographic space is highly fragmented. There are multiple security solutions that utilize cryptography in an inherent way. There are many ways of authenticating people's identity to provide or prevent them access to systems, including passwords, OTP, and smartcards. There are also many protocols to authenticate machines and protect communication between them.

In addition, encryption is needed for databases, VMs, storage, and more, across different clouds and data centers. Furthermore, cryptographic signatures are needed for documents, transactions and code. In many organizations, there are multiple point and siloed solutions that result in management pain, lack of visibility, agility, and flexibility, with high cost to deploy in the different environments that must be supported.

Scoping out a new approach

Today's threat-filled digital landscape requires the enterprise to adopt a new approach to deploying and managing cryptography. It requires a transition on multiple levels:

- **From hardware only to hybrid hardware and software:** Legacy key protection relied solely on hardware solutions. In today's environments where everything is virtualized and much is remote, and enterprises are moving to cloud deployments, pure hardware solutions constitute a significant obstacle. As a result, software solutions for key protection with strong guarantees are needed to replace and complement existing hardware.
- **From siloed to unified key management:** Legacy key protection and management was comprised of different solutions for different environments and business problems. A unified approach with one platform that can support all cryptographic solutions in any environment is needed today.
- **From disparate to integrated key management and key protection:** Legacy key protection provides only basic management and dedicated key management solutions are often not integrated with key protection. A unified platform providing integrated key protection and management is required.
- **From key theft to key misuse prevention:** Legacy key protection solutions address the problem of key theft only. Today, key misuse must be addressed as an integral part of key protection.
- **From rigid to agile infrastructure:** Legacy key protection and management solutions are rigid and slow moving. Cryptography standards are continually changing – updates must be rolled out quickly, new threats considered and resolved. Today's cryptographic infrastructure needs to support agility.
- **From slow to fast deployment:** Legacy cryptographic solutions that relied on solely on hardware were slow to deploy. Today enterprise security teams must offer on-demand cryptographic services internally in order to quickly support business needs.

In modern environments, cryptography is needed everywhere. However, this cannot work if the cryptographic infrastructure in use is the same as in the 1990s. The fragmented legacy cryptographic infrastructure does not support modern business needs and is in desperate need of modernization.

Finding a way forward

The above challenges with legacy key protection and management solutions must be addressed.

- First, modern solutions are needed that are based on openness and transparency and support collaborative environments.
- Second, modern software that works in modern computing environments must be built.
- Third, a new technological approach is required to deliver a software key store with proven security guarantees to complement legacy hardware and support new security requirements.

How can this be achieved? The philosophy behind legacy solutions is to build a fortress around the device that holds key material and prevent any attacker from breaching that machine. In today's zero-trust environments, this is problematic, especially when considering software-only solutions.

A completely different paradigm is to protect cryptographic keys and secrets by never having them reside in any single place at any single time, and to force an attacker to simultaneously breach multiple machines to learn anything. That way there would be no single point of security failure, and strong separations between the different machines would make it extremely hard to breach.

This goal may appear impossible – how can one carry out cryptographic operations such as decryption or signing, without holding the key? Fortunately, a methodology called Secure Multiparty Computation (MPC), also known as threshold cryptography, can do exactly this. Using MPC, the secret key is generated in two or more parts called shares, so that all shares are needed to get any information about the key. These different shares reside on different servers and devices, so that an attacker has to breach them all to steal the key.

MPC protocols enable the different machines holding key shares to interact, so they receive the result of the operation without revealing to each other anything about the key. This means the key remains fully protected, even while in use. MPC protocols have mathematical proofs of security, guaranteeing that an attacker who cannot breach all machines is unable to learn anything about the key, even if they know the protocols used. Although anti-intuitive, when using MPC, the key is never whole in any single place, not when being generated and not while being used.

Implementing a unified solution

What's needed to address these areas is a new platform-based approach to securing enterprise cryptographic infrastructures, one that virtualizes cryptographic key stores and provides a layer of abstraction that delivers cryptographic services to applications, wherever they are: an engine that is a distributed environment that builds a mesh of cryptographic key stores of all types, delivering on-demand cryptographic services at the edge.

Critically too, any such solution must deliver a unified approach to key storage, enabling organizations to enjoy its own features and capabilities while being free to choose the key store best suited to their needs.

By transforming their existing fragmented infrastructure into a unified solution of this kind, organizations attain enhanced efficiency, better security, better user experience and at a lower cost. For any given specific cryptographic problem, it's possible to add a point solution and increase the already fragmented space in the enterprise. Alternatively, a unified solution can be deployed, providing the necessary infrastructure for all cryptographic needs.

By virtualizing cryptography, businesses ensure that their cryptographic infrastructure works the way their other software works. When it is virtual, they can scale it, and they can work in the cloud or on-premises in exactly the same way. It has the benefits of cloud economy, and it's agile. All those benefits can come immediately, automatically and at low cost. Finally, and critically, such solutions facilitate key orchestration across the enterprise and manage all cryptographic devices and solutions from one place. It's a new paradigm, bringing cryptography to the next phase of technological advancement for the enterprise.

02 Jun 2021

46 Optimal teleportation via noisy quantum channels without additional qubit resources

https://www.nature.com/articles/s41534-021-00426-x

Quantum teleportation exemplifies how the transmission of quantum information starkly differs from that of classical information and serves as a key protocol for quantum communication and quantum computing. While an ideal teleportation protocol requires noiseless quantum channels to share a pure maximally entangled state, the reality is that shared entanglement is often severely degraded due to various decoherence mechanisms. Although the quantum noise induced by the decoherence is indeed a major obstacle to realizing a near-term quantum network or processor with a limited number of qubits, the methodologies considered thus far to address this issue are resource-intensive. In the paper, authors demonstrate a protocol that allows optimal quantum teleportation via noisy quantum channels without additional qubit resources. By analyzing teleportation in the framework of generalized quantum measurement, we optimize the teleportation protocol for noisy quantum channels. In particular, they experimentally demonstrate that their protocol enables to teleport an unknown qubit even via a single copy of an entangled state under strong decoherence that would otherwise preclude any quantum operation. Their work provides a useful methodology for practically coping with decoherence with a limited number of qubits and paves the way for realizing noisy intermediate-scale quantum computing and quantum communication.

01 Jun 2021

47 Engineers demonstrate a quantum advantage

by University of Arizona College of Engineering

https://www.sciencedaily.com/releases/2021/06/210601155610.htm

Quantum computing and quantum sensing have the potential to be vastly more powerful than their classical counterparts. Not only could a fully realized quantum computer take just seconds to solve equations that would take a classical computer thousands of years, but it could have incalculable impacts on areas ranging from biomedical imaging to autonomous driving.

However, the technology isn't quite there yet.

In fact, despite widespread theories about the far-reaching impact of quantum technologies, very few researchers have been able to demonstrate, using the technology available now, that quantum methods have an advantage over their classical counterparts.

In a paper published on June 1 in the journal Physical Review X, University of Arizona researchers experimentally show that quantum has an advantage over classical computing systems.

"Demonstrating a quantum advantage is a long-sought-after goal in the community, and very few experiments have been able to show it," said paper co-author Zheshen Zhang, assistant professor of materials science and engineering, principal investigator of the UArizona Quantum Information and Materials Group and one of the paper's authors. "We are seeking to demonstrate how we can leverage the quantum technology that already exists to benefit real-world applications."

How (and When) Quantum Works

Quantum computing and other quantum processes rely on tiny, powerful units of information called qubits. The classical computers we use today work with units of information called bits, which exist as either 0s or 1s, but qubits are capable of existing in both states at the same time. This duality makes them both powerful and fragile. The delicate qubits are prone to collapse without warning, making a process called error correction – which addresses such problems as they happen – very important.

The quantum field is now in an era that John Preskill, a physicist from the California Institute of Technology, termed "noisy intermediate scale quantum," or NISQ. In the NISQ era, quantum computers can perform tasks that only require about 50 to a few hundred qubits, though with a significant amount of noise, or interference. Any more than that and the noisiness overpowers the usefulness, causing everything to collapse. It is widely believed that 10,000 to several million qubits would be needed to carry out practically useful quantum applications.

Imagine inventing a system that guarantees every meal you cook will turn out perfectly, and then giving that system to a group of children who don't have the right ingredients. It will be great in a few years, once the kids become adults and can buy what they need. But until then, the usefulness of the system is limited. Similarly, until researchers advance the field of error correction, which can reduce noise levels, quantum computations are limited to a small scale.

Entanglement Advantages

The experiment described in the paper used a mix of both classical and quantum techniques. Specifically, it used three sensors to classify the average amplitude and angle of radio frequency signals.

The sensors were equipped with another quantum resource called entanglement, which allows them to share information with one another and provides two major benefits: First, it improves the sensitivity of the sensors and reduces errors. Second, because they are entangled, the sensors evaluate global properties rather than gathering data about specific parts of a system. This is useful for applications that only need a binary answer; for example, in medical imaging, researchers don't need to know about every single cell in a tissue sample that isn't cancerous – just whether there's one cell that is cancerous. The same concept applies to detecting hazardous chemicals in drinking water.

The experiment demonstrated that equipping the sensors with quantum entanglement gave them an advantage over classical sensors, reducing the likelihood of errors by a small but critical margin.

"This idea of using entanglement to improve sensors is not limited to a specific type of sensor, so it could be used for a range of different applications, as long as you have the equipment to entangle the sensors," said study co-author Quntao Zhuang, assistant professor of electrical and computer engineering

and principal investigator of the Quantum Information Theory Group. “In theory, you could consider applications like lidar (Light Detection and Ranging) for self-driving cars, for example.”

Zhuang and Zhang developed the theory behind the experiment and described it in a 2019 Physical Review X paper. They co-authored the new paper with lead author Yi Xia, a doctoral student in the James C. Wyant College of Optical Sciences, and Wei Li, a postdoctoral researcher in materials science and engineering.

Qubit Classifiers

There are existing applications that use a mix of quantum and classical processing in the NISQ era, but they rely on preexisting classical datasets that must be converted and classified in the quantum realm. Imagine taking a series of photos of cats and dogs, then uploading the photos into a system that uses quantum methods to label the photos as either “cat” or “dog.”

The team is tackling the labeling process from a different angle, by using quantum sensors to gather their own data in the first place. It’s more like using a specialized quantum camera that labels the photos as either “dog” or “cat” as the photos are taken.

“A lot of algorithms consider data stored on a computer disk, and then convert that into a quantum system, which takes time and effort,” Zhuang said. “Our system works on a different problem by evaluating physical processes that are happening in real time.”

The team is excited for future applications of their work at the intersection of quantum sensing and quantum computing. They even envision one day integrating their entire experimental setup onto a chip that could be dipped into a biomaterial or water sample to identify disease or harmful chemicals.

“We think it’s a new paradigm for both quantum computing, quantum machine learning and quantum sensors, because it really creates a bridge to interconnect all these different domains,” Zhang said.

48 Quantum algorithm provides new approach to NP-hard problem

by Lisa Tse

https://physicsworld.com/a/quantum-algorithm-provides-new-approach-to-np-hard-problem/

Imagine a parallel universe where physicists are remunerated so handsomely that they can accumulate multitudinous assets. In this alternate universe, you naturally wish to share your good fortune, so you decide to divide your assets equally between your two non-physicist friends. This is an example of the number partitioning problem, in which the aim is to partition a single list of integers into two balanced lists in a way that minimizes the discrepancy between the sums of each list. In this example, the integers correspond to the values of your assets and the balanced lists represent the assets going to each friend.

Your enthusiasm wanes, however, when you find out that this seemingly simple task is notoriously hard. In fact, the number partitioning problem is classed as NP-hard, meaning that an optimal solution is difficult to find but easy to verify.

Researchers at Stanford University have now developed a quantum approach. By applying a well-established quantum algorithm known as Grover’s algorithm to the number partitioning problem, they obtain a quadratic speedup compared to equivalent classical algorithms. The team also proposes a way to implement this algorithm in near-term quantum devices such as those using cold atoms.

General approach

Grover's algorithm is designed to find a specific item in a database, and it relies on a so-called oracle to judge whether a given item is the target of the search. Once each item in the database is encoded as a distinct quantum state, the next step is to construct an equally weighted superposition of these states. After that, the oracle is applied to the superposition so that it imparts a phase difference on the quantum state that encodes the target item. This marks the target, after which its probability of being measured can be boosted. The process is then applied repeatedly until the measurement probability is sufficiently high.

The Stanford researchers apply Grover's algorithm to the number partitioning problem by encoding each possible partition of the integer list as a quantum state. They also formulate an oracle that can identify an optimal partition, which is possible because solutions of NP-hard problems are easy to verify. Grover's algorithm then searches for an optimal partition.

To implement the algorithm, the physicists propose a hardware architecture in which a central quantum spin (such as a Rydberg atom) or a central boson (such as a bosonic mode from a cavity) is coupled to all the other spins in the system, with no other couplings present. This arrangement is known as a star graph (see image). The central entity acts as the oracle, and its coupling strengths to the other spins represent the integers in the list.

Future directions

"Our proposal opens the possibility of implementing Grover's algorithm efficiently on devices before full quantum error correction is achieved, improving the prospects of tackling real-world problems on these near-term devices," says Ognjen Marković, a co-author of the study.

Marković also believes that this work could stimulate research in the field of quantum-classical hybrid algorithms. For instance, the team's proposed implementation of Grover's algorithm could be used as a quantum subroutine in a larger, possibly classical algorithm.

49 Ending encryption: On enforcing traceability on popular messaging apps

https://www.thehindu.com/opinion/editorial/ending-encryption-on-enforcing-traceability-on-popular-messaging-apps/article34693043.ecehttps://theconversation.com/declassified-cold-war-code-breaking-manual-has-lessons-for-solving-impossible-puzzles-161595

Barely a day before the Information Technology Rules 2021 came into force, WhatsApp moved the Delhi High Court against the rules – specifically the one that mandates that a "significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order". Given the specification that a "significant social media intermediary" is one with more than 50 lakh registered users, WhatsApp's messenger service would clearly be affected. WhatsApp's contention is that for compliance and traceability, it would have to break its end-to-end encryption service that allows messages to be read only by the sender and the receiver. Its argument is that the encryption feature allows for privacy protections and breaking it would mean a violation of privacy. The question to be asked is whether the traceability

guidelines (by breaking encryption) are vital to law enforcement in cases of harmful content. A release by the Ministry of Electronics and IT has said that the traceability measure will be used by law enforcement as the "last resort" and will come by only in specific situations, such as "for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India ... or child sexual abuse material, punishable with imprisonment ..." The assertion suggests that this requirement is in line with the Puttaswamy judgment that clarified that any restriction to the right of privacy must be necessary, proportionate and include safeguards against abuse.

But the Government, as the law stands now, can already seek access to encrypted data under Section 69(3) of the IT Act, and Rules 17 and 13 of the 2009 Surveillance Rules that require intermediaries to assist with decryption when they have the technical ability to do so and when law enforcement has no other alternative. Besides, it can still seek unencrypted data, metadata and digital trails from intermediaries such as WhatsApp. The trouble with enforcing traceability is that without safeguards such as having any independent or judicial oversight, government agencies could seek any user's identity on vague grounds and this could compromise the anonymity of whistle-blowers and journalistic sources, who can claim to be acting in the public interest. WhatsApp's contention that "requiring messaging apps to 'trace' chats is the equivalent of asking us to keep a fingerprint of every single message sent ... and fundamentally undermines right to privacy" is, therefore, not hyperbole. If anything, the Government needs to revisit its position on traceability commitments of intermediaries and instead revise the IT Act, 2000 in line with existing global best practices besides legislating the long-pending Data Protection Bill.