Crypto News

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

August 01, 2022

1.Editorial

It's August and what a fantastic summer month to sit by the pool and read this month's Crypto News! We all know the old adage that reading can take your mind to fantastic new places and teach you new information at the same time. So, let's start our journey with article #3 and take a trip to India to learn about what they are planning as it relates to quantum computing. This article walks through India's current challenges with quantum computing and their initiatives. Between the National Mission on Quantum Technologies and Applications, QuEST, and the Department of Space initiatives, they are well on their way to a successful path forward as it relates to quantum computing.

Next, let's head over to the United States of America in articles #24 and #25 which report on the news many have been waiting on: the rollout of the NIST encryption standards. The four selected encryption algorithms will be a part of the NIST PQC standard expected to be released in the near future. Let's stay in the United States and hop to article #13 and explore what the NSA is doing to safeguard themselves against the inevitable future in which quantum computers will be "used against the digital infrastructure that safeguards" their most sensitive data. With an expedited timeline to finalize PQC standards due to NSM-8 being signed by President Biden in January 2022, the NSA is working quickly with other agencies and encouraging public-private collaboration. Private organizations also need to plan for and move towards post-quantum encryption to properly protect data entrusted to them for safe keeping. What is your organization doing to prepare for the post quantum world?

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

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

2.Researchers create key tech for quantum cryptography commercialization

by Help Net Security
https://www.helpnetsecurity.com/2022/07/29/quantum-cryptography-commercialization/

In modern cryptosystems, users generate public and private keys that guarantee security based on computational complexity and use them to encrypt and decrypt information. However, recently, modern public-key cryptosystems have faced potential security loopholes against quantum computers with great computational power.

As a solution, quantum cryptosystems have been highly noticed. They use quantum keys that guarantee

security based on quantum physics rather than computational complexity, thus they are secure even against quantum computers. Therefore, quantum cryptosystems are expected to replace modern cryptosystems.

Quantum key distribution (QKD) is the most important technology for realizing quantum cryptosystems. Two main technical issues should be addressed to commercialize QKD. One is the communication distance, and the other is the expansion from one-to-one (1:1) communication to one-to-many (1:N) or many-to-many (N:N) network communication.

Twin-field (TF) QKD, announced in 2018, is a long-distance protocol, which can dramatically increase the communication distance of QKD systems. In TF QKD, two users can distribute a key by transmitting quantum signals to an intermediate third-party that is for measurement. Given the inevitable channel loss, this architecture allows the users to increase the communication distance. However, despite its innovativeness, it has been experimentally demonstrated by only a few global QKD leading groups owing to the significant difficulty of system implementation, and research on the TF QKD network is still insufficient.

The Korea Institute of Science and Technology (KIST) announced that their research team, the Center for Quantum Information, led by director Sang-Wook Han, succeeded in an experimental demonstration of a practical TF QKD network. This is the second experimental demonstration of the TF QKD network in the world after the University of Toronto in Canada.

The research team proposed a new TF QKD network structure scalable to a two-to-many (2:N) network based on polarization-, time-, and wavelength-division multiplexing. Unlike the first demonstration of the University of Toronto based on a ring network structure, the research team's architecture is based on a star network. The quantum signal in a ring structure must pass through every user connected to the ring, however, the star structure only has it go through the center, making it possible to implement a more practical QKD system.

Besides, to overcome the main implementation obstacles to developing the TF QKD system, the team applied a plug-and-play (PnP) structure. A conventional TF QKD system requires many control systems, such as timing, wavelength, phase, and polarization controllers, to maintain the indistinguishability of two quantum signals emitted by two users' different light sources.

Whereas in the PnP TF QKD architecture developed by the KIST research team, the middle third-party generates and transmits the initial signals to both users using a single light source, and the signals return to the third-party by making a round trip. Therefore, the polarization drift due to the birefringence effect of the channel is automatically compensated, and users have fundamentally the same wavelength.

In addition, due to the two signals passing through the same route in opposite directions, the arrival times of the signals are naturally identical. As a result, only a phase controller is required for implementing the research team's architecture. Based on the architecture, the team successfully conducted an experimental demonstration of a TF QKD network.

"It is a significant research achievement showing the possibility of solving the two main obstacles to

QKD commercialization, and we have gained a key technology leading the corresponding research," said Sang-Wook Han, the leader of the Center for Quantum Information.

3.Quantum Computing: Uses, Challenges and India's Initiatives – Explained, point-wise

by Kunal Khureja
https://blog.forumias.com/quantum-computing-uses-challenges-and-indias-initiatives/

Introduction

The 21st century will be an era of cutting edge technology that will enable humans to achieve the hitherto impossible tasks. Amongst these game changing technologies, a critical role would be played by quantum computing and technology. Quantum computing is an emerging field of physics and engineering, which relies on the principles of quantum physics (the physics of subatomic particles). It promises improvements to a vast range of everyday technology. It will enable the nations to strengthen their economic, social and military might owing to the multifarious applications of quantum computing in areas like health, education, defense, manufacturing etc. India is on the right path to leverage this technology but realizing its true potential warrants some more focused efforts from the Government as well as the private sector.

What is Quantum Computing?

It is a type of computation that harnesses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations. It harnesses the phenomena of quantum mechanics to deliver a huge leap forward in computation to solve complex problems.

Quantum mechanics is a science that describes the unique behavior of matter and energy at the atomic and subatomic level.

Quantum Computing works on:

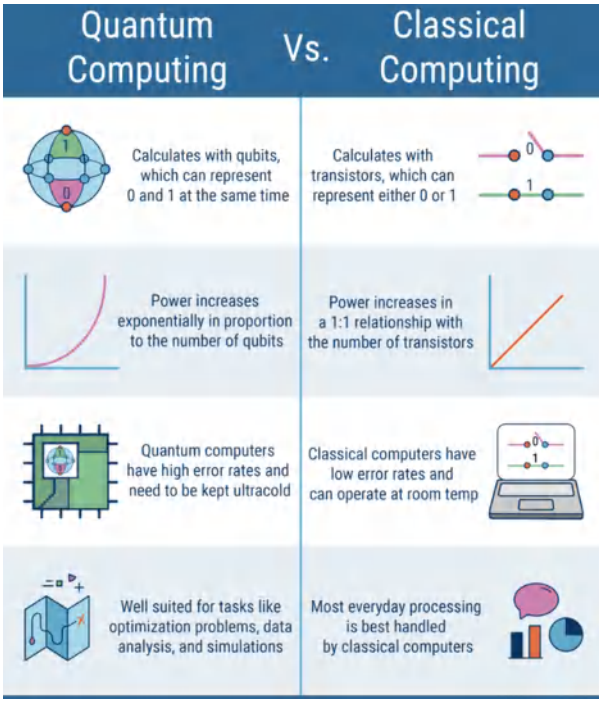
'Superposition' meaning they can exist in multiple states (both 0,1 at the same time) at the same time. It is unlike classical computers where information is processed in 'bits' or 1s and 0s, following classical physics.

'Entanglement' where two or more particles are inextricably linked and mirror each other exactly, even when separated by great physical distance.

How are Quantum Computers better than Conventional Supercomputers?

Conventional computers (in common use like homes/offices) and Supercomputers process information with **bits** (ones and zeroes). Quantum computers, on the other hand, use quantum bits or **qubits** that can process the ones and zeroes simultaneously due to a property known as superposition. This allows them to process a lot more information than conventional computers

Conventional Supercomputers combine processing power of thousands of computers. However, supercomputers aren't very good at solving certain types of problems e.g., Supercomputers don't have the working memory to hold the myriad combinations of real world problems. Supercomputers have to analyze each combination one after another, which can take a long time.



On the other hand, the computing power of quantum computers increases exponentially (by a factor of 2) with increase in qubits e.g., In October 2019, Google said it had performed a calculation on a quantum processor in 300 seconds that would have been **practically impossible** to achieve with the algorithms available at the time.

What are the various applications of Quantum Computing?

Artificial Intelligence (AI) and Machine Learning (ML): Quantum computers' abilities to parse through massive data sets, simulate complex models, and quickly solve optimization problems have drawn attention for applications within artificial intelligence. Quantum computing has the potential to enhance the pace of AI/ML.

Computational Chemistry: There are many problems in finding the right catalyst or process to develop a new material, or an existing material more efficiently. A quantum computer can be used to simulate the quantum mechanical processes that occur. Potential applications include: **(a)** Finding new materials that can achieve a room temperature superconductor; **(b)** Finding a catalyst that can improve the ef-

ficiency of carbon sequestration; **(c)** Developing a new battery chemistry that can significantly improve the performance over today's lithium-ion batteries.

These applications can have uses in agriculture, manufacturing and industrial design sectors.

Financial Portfolio Optimisation: Finding the optimum mix for a basketful of investments based upon projected returns, risk assessments, and other factors is a daily task within the finance industry. By utilizing quantum technology to perform these calculations, improvements can be achieved in both the quality of the solutions as well as the time to develop them.

Logistics and Scheduling: Many common optimisations used in industry can be classified under logistics and scheduling. Quantum computing can make logistics more efficient. For example: **(a)** Airlines can figure out how to stage their airplanes for the best service at the lowest cost; **(b)** Factory managers can minimize cost, time and maximize output.

Cyber Security: Cyber security is becoming a larger issue every day as threats around the world are increasing their capabilities and we become more vulnerable as we increase our dependence upon the digital system. Various techniques to combat cyber security threats can be developed using some of the quantum machine learning approaches to recognize the threats earlier and mitigate the damage that they may do.

Why should India focus on Quantum Computing?

Industrial revolution 4.0: Quantum computing is an integral part of Industrial revolution 4.0. Success in it will help in Strategic initiatives aimed at leveraging other Industrial revolution 4.0 technologies like the Internet-of-Things, Machine Learning, robotics, and artificial intelligence across sectors and lay the foundation of the Knowledge economy.

Growing Demand: According to the The Quantum Revolution in India, The quantum ecosystem in India is growing at an accelerated pace with support from government agencies and participation from the academia, service providers, and the start-up community.

Economic Benefits: The adoption of quantum technologies across industries could potentially add US$ 280–310 billion value to the Indian economy by 2030. Manufacturing, high-tech, banking, and defence sectors will remain at the forefront of quantum-led innovation, according to the Nasscom-Avasant report.

What steps have been taken to promote Quantum Computing in India?

The National Mission on Quantum Technologies and Applications (NM-QTA): It is a government of India programme that aims to create a workforce of over 25,000 in India over the next 5-7 years. It has a total budget outlay of ₹8,000 crore for a period of five years.

The next generation transformative technologies that will receive a push under this mission include quantum computers and computing, quantum communication, quantum key distribution, encryption, quantum devices, quantum sensing and so on.

The areas of focus for the Mission will be in fundamental science, translation, technology development, human and infrastructural resource generation, innovation and start-ups to address issues concerning national priorities.

QuEST: The Department of Science and Technology launched the Quantum-Enabled Science and Technology (QuEST) initiative to invest INR 80 crores to lay out infrastructure and to facilitate research in the field.

'Quantum Computer Simulator (QSim) Toolkit': It provides the first quantum development environment to academicians, industry professionals, students, and the scientific community in India.

Other Efforts: Scientists from two Ahmedabad-based laboratories of the Department of Space jointly demonstrated quantum entanglement with real-time Quantum Key Distribution (QKD) between two buildings separated by a distance of 300 metres.

What are the associated challenges?

First, quantum computers are highly prone to interference that leads to errors in quantum algorithms running on it. Thus it can give erroneous results. Scientists are working to improve accuracy e.g., Google has announced plans to have fault-tolerant quantum-computing hardware by 2030

Second, most quantum computers cannot function without being super-cooled to a little above absolute zero since heat generates error or noise in qubits. Expanding quantum computing will increase ecological footprint.

Third, finding the right talent is another big hurdle as there is an acute shortage of candidates with doctorates in quantum physics, engineering, and statistics.

Fourth, a comprehensive multi-stakeholder network is amiss. It is not clear whether India will focus on near-term quantum applications or long-term applications or both. Translating research into real-world applications should be at the core of India's quantum efforts.

Fifth, metrics to assess the outcomes of India's quantum efforts are not clearly defined. Merely achieving quantum supremacy will not necessarily safeguard India's national interests.

Sixth, India lacks the capability to domestically manufacture most of the components/hardware used in quantum computing. It is another strategic sector where India is import-dependent.

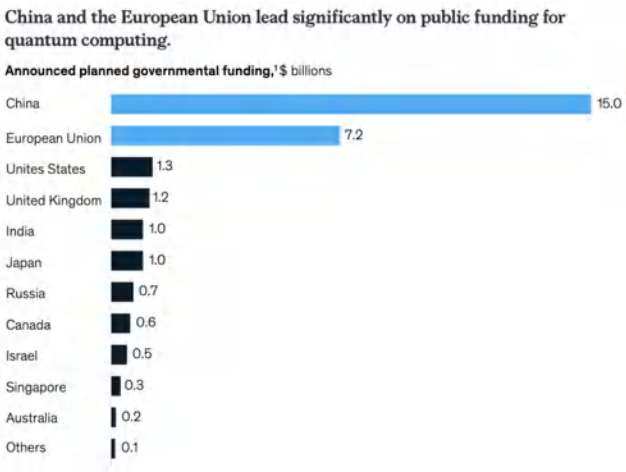
What should be the approach going ahead?

First, India should cooperate with the private sector and friendly nations who are working to address the critical bottlenecks of quantum computing e.g., Tech Mahindra's research and development arm, Makers Lab, announced it has set up a quantum centre of excellence called QNxT in Finland to leverage the country's expertise in quantum computing.

Second, the Indian government had announced NM-QTA in 2020 but it is yet to get Cabinet clearance. This should be quickly approved and implemented.

Third, the Government should also make sure that educational programs surrounding quantum computing and technology are provided with adequate support and completed on time e.g., the Defence Institute of Advanced Technology (DIAT) in Pune, launched an MTech in quantum computing in 2020. IBM has partnered with top-tier academic institutions in India to provide access to IBM quantum systems, while Microsoft Garage India has joined hands with IIT Roorkee to conduct lectures on quantum computing for an entire semester.

Fourth, the funding support towards the technology also needs to be augmented. According to McKinsey, China and the European Union have taken a lead in public funding for quantum computing with investments worth US$ 15 billion and US$ 7.2 billion, respectively. The US, the UK and India follow but with much lesser spending.



Conclusion

Despite these hurdles, quantum computing is set to grow. It is likely to see a hybrid computing-operating model that combines conventional computing with emerging quantum computing before the latter comes of age. Change may come as early as 2030, as several companies predict they will launch usable quantum systems by that time. India must step-up the efforts to develop capabilities in quantum computing and technologies. China has already gained a significant lead in this strategic field, India must catch-up before the gap with China's capabilities becomes too wide to plug.

4.Hack Post-Quantum Cryptography Now So That Bad Actors Don't Do It Later

by Edward Parker & Michael Vermeer

https://www.lawfareblog.com/hack-post-quantum-cryptography-now-so-bad-actors-dont-do-it-later

In February, a researcher sent a shock wave through the cryptography community by claiming that an algorithm that might become a cornerstone of the next generation of internet encryption can be cracked mathematically using a single laptop. This finding may have averted a massive cybersecurity vulnerability. But it also raises concerns that new encryption methods for securing internet traffic contain other flaws that have not yet been detected. One way to build trust in these new encryption methods—and to help catch any other weaknesses before they are deployed—would be to run a public contest to incentivize more people to look for weaknesses in these new algorithms.

The new encryption algorithm that was just cracked was designed to be secure against quantum computers. A large-scale quantum computer may eventually be able to quickly break the encryption used to secure today's internet traffic. If internet users don't take any countermeasures, then anyone in possession of such a computer might be able to read all secure online communications—such as email, financial transactions, medical records, and trade secrets—with potentially catastrophic impacts for cybersecurity that the U.S. National Security Agency has described as "devastating to … our nation."

One defense against this future threat is post-quantum cryptography or PQC—a set of new cryptography algorithms that are expected to resist attacks from quantum computers. Since 2015, the U.S. National Institute for Standards and Technology (NIST) has been evaluating algorithms to design a new standard for this type of cryptography, which will likely be adopted eventually by communication systems worldwide. Although quantum computers powerful enough to threaten encryption are unlikely to arrive before 2030, upgrading to PQC will take years and cost billions of dollars. The U.S. government considers the swift and comprehensive adoption of PQC across its own communication systems to be an important national security imperative: Over the past two months, the White House has issued a National Security Memorandum directing all federal agencies to begin preparing for the transition. And related bills have passed the House of Representatives and been introduced in the Senate with bipartisan support.

If a deployed PQC algorithm contained a security flaw, an enormous amount of sensitive information could be left vulnerable. And there could be a chaotic and costly scramble to fix the flaw throughout the communication infrastructure. The recent claim to have found just such a flaw in one of the PQC algorithms that NIST was considering shows that this risk is not far-fetched.

NIST and others in the cryptography community are carefully analyzing several PQC algorithms to try to catch any potential vulnerabilities. But it's almost impossible to mathematically prove the security of most cryptography algorithms. In practice, the strongest evidence for an algorithm's security is simply that many experts have tried and failed to break it. The more people try to attack the new PQC algorithms and fail, the more likely it is that they are secure.

One possible option for further crowdsourcing the analysis of NIST's final candidate PQC algorithms would be a contest in which the general public is invited to try to break them. As hundreds of companies that offer public bug bounties have discovered, crowdsourced penetration testing can be a very useful tool for improving cybersecurity. The U.S. Departments of Homeland Security and Defense have also recently experimented with offering bug bounties to anyone who discovers cyber vulnerabilities in the departments' systems. A public contest certainly can't replace a mathematical security analysis,

but it could be a useful complement that provides additional evidence of the algorithms' security.

Here's one possible option for what such a contest might look like: NIST could use its recently selected candidate PQC algorithms to encrypt a nonsensitive document and then publicly release the encrypted ciphertext (and the algorithms used to encrypt it) along with a large bounty for its decryption. The first person—anywhere in the world—to successfully decrypt the document and explain how they did so would receive the bounty. If anyone succeeds, NIST would know that it needs to refine its algorithms before releasing the final standard.

One of the main advantages of a high-profile contest is that it would enable the examination of the candidate algorithms from fresh perspectives. NIST's standardization process has been quite transparent. But PQC is still an esoteric and highly technical topic, and relatively few people have carefully studied NIST's chosen algorithms. A public contest might attract more cryptographers and others with a wider variety of backgrounds, including enthusiasts, white-hat hackers, and anyone who would appreciate the opportunity to publicly "pwn the government" by defeating its proposed cryptography systems (in addition to winning a substantial financial prize).

There are several potential objections to this proposal. The first is that previous cryptography cracking contests have often failed to be very effective. But cryptography cash bounties have also been successfully offered. As long as this contest is carefully designed, it can avoid the common pitfalls of previous contests. For example, the contest would need to offer a large enough prize to incentivize significant effort, the PQC algorithm(s) used would need to be clearly specified, and there would need to be few constraints on which tools the participants are allowed to use.

A second objection is that such a contest could backfire. If it incentivizes participants to discover a vulnerability, they could potentially decide to exploit or sell the vulnerability rather than disclosing it to the contest sponsor and claiming the bounty. This outcome is conceivable, but unlikely. Most people who would be incentivized on the margin by this contest would likely be hobbyists or academics rather than professional black-hat hackers, and they are unlikely to be either willing or able to exploit or sell a serious vulnerability. If a financially motivated person does discover a vulnerability, then a cash bounty would create an incentive for them to disclose it to the U.S. government instead of exploiting or selling it. Also, if multiple people discover the same vulnerability, only a single person would need to disclose it in order for the contest to succeed—and it's unlikely that every single person who discovers the vulnerability would choose to misuse it. More generally, the broad cryptography principle known as Shannon's maxim—"the enemy knows the system"—favors rapidly uncovering and fixing any fundamental weaknesses in cryptography systems, rather than counting on those vulnerabilities to remain undiscovered by adversaries.

A third objection is that organizing such a contest would be a waste of effort, because participants would be unlikely to uncover any vulnerabilities that the professional mathematicians at NIST have missed after years of work. It's true that the bounty would (fortunately) probably never need to be paid out. But the contest could be valuable whether or not it ever awards a prize. Its mere existence might reassure the business community—which is more familiar with the notion of bug bounties than with the kind of formal cryptographic analysis that NIST is carrying out—that these new PQC algorithms are secure. The authors previously recommended that the government look for innovative ways to spur the rapid adoption of PQC. Assuring organizations of the security of the PQC standard is one

way to do so. Moreover, a contest would raise public awareness of PQC and would encourage participants to dig into the mathematical details. An increase in public familiarity with PQC (at all levels of technical detail) could generate broad cybersecurity benefits for years to come.

It may seem counterintuitive to directly incentivize people to break cryptography that will eventually be used by government and commercial organizations. But given the incredibly high stakes of the transition to PQC, it's absolutely critical that NIST receive every possible assurance that these algorithms are secure. If the new PQC algorithms do turn out to contain vulnerabilities like the recently discovered one, then it would be much better to find those vulnerabilities before the algorithms are rolled out widely. These PQC algorithms will eventually become the bedrock of cybersecurity for the entire internet. If a bounty helps to catch a vulnerability before it's deployed, then the modest cost of the bounty could prevent much higher costs further down the line.

5.Hiding Secrets Using Quantum Entanglement

by Sophia Chen
https://physics.aps.org/articles/v15/116

Three experiments demonstrate the key elements of a quantum cryptographic scheme that predictions indicate should be unhackable, bringing the promise of quantum encryption technologies a step closer to reality.

In the 1980s, physicists began proposing quantum-based encryption methods that would scramble data to guarantee its security. The methods exploit a particular quirk of quantum systems: that measurements of those systems inherently change the systems' properties. Specifically, the protocols involve serial measurements of quantum objects, the statistics of which should reveal any eavesdropper. However, researchers have struggled to build devices that work exactly as the protocols specify. Now three research groups, one based in Germany, one in the UK, and one in China, have independently performed proof-of-principle experiments of a quantum encryption method that can secure information even if the devices used do not behave exactly as predicted [1–3]. The demonstrations are "a major breakthrough for cybersecurity," says Charles Lim of the National University of Singapore, who was involved in the Germany-based experiments.

The three experiments each demonstrate aspects of an encryption method known as device-independent quantum key distribution (DIQKD). In DIQKD, a device repeatedly generates pairs of entangled quantum particles. Two parties, Alice and Bob, each take one particle from every pair. Alice and Bob then create a "key"—a string of 1's and 0's that can encode and decode messages—in part by making a series of measurements of a two-outcome property of their particles. If the particle is a photon, this property might be its polarization, which can be horizontal or vertical. For an atom, it might be the atom's state (ground or excited). Because the outcome of a measurement on one particle is correlated with that of its entangled counterpart, Alice and Bob can generate a single shared key after some postprocessing.

As Alice and Bob make these measurements, they intermittently verify the security of their channel using a test based on a quantum rule known as Bell's theorem. According to Bell's theorem, if two particles are entangled, measurements of those particles must exhibit specific statistical correlations. For the test, Alice and Bob use a subset of the measurements for generating the key. They then check that the measurements follow the prescribed statistics. If there is a mismatch, Alice and Bob know that their particles are no longer entangled, indicating that they can no longer guarantee the security of the channel. They then discard their measurements and restart the process.

Researchers have mathematically proven the security of DIQKD. No such proof exists for standard classical encryption methods, which rely on the computational difficulty of factoring large numbers. Researchers anticipate that future quantum computers will be able to quickly factor these numbers, rendering current classical encryption obsolete. On the other hand, DIQKD provides security "against an adversary with arbitrary processing power or even a quantum computer," says Jean-Daniel Bancal of the French National Center for Scientific Research (CNRS).

For the DIQKD methods used in the new experiments, Alice and Bob require no information about the device that generated their particles, meaning that researchers "don't need to model [their] devices," says Antonio Acín of the Institute of Photonic Sciences in Spain, who was not involved in any of the experiments. "You can treat them as black boxes." Thus, the methods sidestep the vulnerabilities of other quantum encryption protocols, some of which have been implemented in commercially available technologies, such as one available from the Swiss company ID Quantique. In 2007, the Swiss government used ID Quantique's encryption devices to secure the votes in their national election. But by 2010, two teams of researchers had successfully hacked ID Quantique's device using discrepancies between its operation and its theoretical description. One team, for example, intercepted an encryption key without either Alice or Bob noticing by exploiting a time gap in the machine's production of successive photons, which theory requires be produced without delay.

"A real device is different from a mathematical model," says Qiang Zhang of the University of Science and Technology of China, a member of the China-based team. "Without full knowledge of that difference, it may leave a backdoor open to an attack."

While the three experiments used similar DIQKD methods, they have notable differences. The China-based experiments used entangled photons; the UK ones, entangled strontium ions; and the German ones, entangled rubidium atoms. "Each has its own advantage," Zhang says. When using atoms and ions, for example, researchers can keep track of both particles in an entangled pair, he says. They have no way of tracking two entangled photons. When one photon in a pair gets lost, this raises other experimental requirements for security, which Zhang's team was able to meet. However, photons are used in many exisiting communications technologies, for example, potentially making it easier and quicker to implement quantum techniques with photons, Zhang says.

Only the UK-based experiment completed an entire DIQKD protocol, generating a 95,000-bit encryption key over about 8 hours. The Germany-based experiment produced a few thousand bits over two days, enough for a small fraction of a key, but it did not complete the key because of time constraints. The China-based experiment also did not generate a complete key because their detector could not keep track of enough entangled photon pairs to do so. Once they improve their detection

efficiency, the team says that their system should only take a few minutes to make a key.

In all the experiments, Alice and Bob were much less than a kilometer apart. In China they were 20 to 220 m apart, in Germany 400 m apart, and in the UK they were separated by only 2 m. Because of those distance limitations, the demonstrations do not yet show that DIQKD can be a practical technology, says Acín. For that to happen, researchers will need to demonstrate the viability of the methods over kilometer-scale distances. They also need the methods to generate keys faster, Lim says.

Given these engineering challenges, Zhang thinks that commercial DIQKD encryption tools are unlikely anytime soon. But he still thinks that the new demonstrations have value. "It [seems like] a ridiculous thing," he says. But these experiments show that "you can use a device that you don't trust, and you can still generate a secure key."

References

1. W. Z. Liu et al., "Toward a photonic demonstration of device-independent quantum key distribution," **Phys. Rev. Lett. 129, 050502 (2022)**.
2. D. P. Nadlinger et al., "Experimental quantum key distribution certified by Bell's theorem," **Nature 607, 682 (2022)**.
3. W. Zhang et al., "A device-independent quantum key distribution system for distant users," **Nature 607, 687 (2022)**.

6.Senators Introduce Quantum Encryption Preparedness Law

by Danny Bradbury

https://www.infosecurity-magazine.com/news/senators-quantum-encryption-law/

A bill to help secure US government cryptographic systems against attack from quantum computers has passed the House and has now advanced to the Senate. The Quantum Computing Cybersecurity Preparedness Act introduces requirements for federal agencies to identify systems using cryptography and prioritize them for migration.

The Act, co-sponsored by senators Rob Portman (R-OH) and Maggie Hassan (D-NH), calls for every executive agency to create an inventory of all the cryptographic systems in use, along with the IT systems that they will prioritize for migration to post-quantum cryptography. They will also define processes for evaluating the process of that migration.

The Office of Management and Budget (OMB) also has a role under the Act. Within 15 months of the law coming into effect, the OMB must create a strategy to manage the risk posed by quantum encryption, along with a report on the funding that executive agencies need to protect themselves.The House version of this Act, sponsored by representatives Ro Khanna (D- CA-17), Gerry

Connolly (D-VA-11), and Nancy Mace (R-SC-1), passed this month after its introduction in April. It was endorsed by Google, IBM, PQSecure Technologies, QuSecure, Maybell Quantum, Quantinuum and Qryp.

Lawmakers introduced the bill because they're worried about the potential for quantum computers to easily crack current cryptographic algorithms. Cryptography typically requires an attacker to conduct many calculations to crack a code. The more bits an encryption key has, the more calculations are required.

Traditional computers use conventional electronic bits to represent numbers. These bits have a binary state (0 or 1), meaning they can only represent one number at a time. This limits them to calculating possible results consecutively. Even with parallel processing, the computing power required to crack modern cryptography algorithms is still prohibitive in many cases.

Conversely, quantum computers use qubits, which are quantum bits exploiting the quantum quality of superposition. This allows them to maintain several states at once, increasing their ability to make different calculations concurrently. These computers could threaten traditional cryptographic algorithms in five to 10 years.

Quantum encryption uses new encryption methods to produce unpredictable encryption keys that these new computers will not easily be able to crack.

America's security services have been aware of the threat for a while. The Department of Homeland Security released a roadmap on PQC in October and the NSA is also working on solutions.

Agencies must provide their inventories of cryptographic systems no later than one year after NIST publishes post-quantum cryptography standards. NIST hasn't finalized these standards yet. It expects to do that within two years. However, this month it did choose four encryption tools that could potentially withstand attacks from a quantum computer.

7.Quantum Technology: Our Sustainable Future—One Year On

by JAMES DARGAN
https://thequantuminsider.com/2022/07/27/quantum-technology-our-sustainable-future-one-year-on/

Last summer, The Quantum Insider released the documentary Quantum Technology | Our Sustainable Future, developed in partnership with Oxford Instruments NanoScience.

Produced as a call from industry experts to discuss the potential of quantum technology in addressing the world's urgent sustainability challenges, it included interviews with many of the leading minds in quantum:

- Alan Ho: Head of Product, Google Quantum AI

- Alexandre Blais: Advisory Board, Q4Climate
- Carl Williams: Deputy Director, Physical Measurement Laboratory at NIST
- Flaviu Cipcigan: Research Staff Member, IBM Research
- Hui Zhang: General Manager, Origin Quantum
- Ilana Wisby: CEO, Oxford Quantum Circuits
- Jingen Xiang: CEO, SpinQ
- John Levy: CEO, SEEQC
- Nicolas Sawaya: Research Scientist, Intel Labs
- Pete Shadbolt: CSO, PsiQuantum
- Richard Murray: CEO, ORCA Computing
- Stuart Woods: Managing Director, Oxford Instruments NanoScience
- Tamar Eilam: IBM fellow, IBM's Thomas J Watson Research Centre

During the thirty-minute documentary, some interesting conclusions were made by the experts who participated:

"I think it's a sign of the times that, despite the broad range of potential applications for quantum computing, so many groups are specifically focused on climate change," said Pete Shadbolt, Chief Strategy Officer at PsiQuantum. "It's inspiring to see the business community prioritize climate applications and acknowledge the gravity of the climate situation we are now in."

John Levy, CEO of SEEQC, said: "We recognize the centrality of sustainability in the development of quantum systems, both from an energy efficiency perspective as well as with the applications that quantum computers will address in areas such as climate modelling, material science and energy. We are pleased to participate in this important documentary with our colleagues in the quantum space to highlight our collective work on a global scale."

It is now nearly a year on from this and The Quantum Insider wanted to see what developments have been made in the twelve months since.

REPORT FINDINGS AND EVENTS

Back in May of this year, McKinsey released an article called Quantum computing might just save the planet. In it, the publication stated that quantum computing could assist in the development of climate technologies that would decrease carbon on the order of 7 gigatons a year of additional CO2 impact by 2035—bringing the world in line with the 1.5°C target.

The article concluded that, though quantum technologies are in the early stage, an unknown proposition and expensive to implement, risks to investors can be reduced through the hiring of technical experts "to run in-depth diligence, forming joint investments with public entities or consortia, and investing in companies that bundle various ventures under one roof and provide the necessary experience to set up and scale these ventures."

At the Economist Impact "Commercialising Quantum" conference this year, sustainability was a hot topic on the second "virtual" day, with several keynote speeches by industry experts. These included:

- How much of a driver is climate change in the current scope of quantum development? Have we got our priorities right?—by Dr. Juan Bernabé-Moreno, Chief data officer, E.ON
- Delivering a quantum leap on climate change: how ambition and cooperation can keep "1.5 alive" —by Dr. Marko Rančić, Head of quantum computing, TotalEnergies
- Exploring the scope of the opportunity for quantum in the hydrogen economy: methane detection and more—by Robin Yellow, Digital science principal, BP#

QUANTUM CONTROVERSY

The increasing interest in quantum technologies relevant for the climate has created a degree of disagreement in the community. On the one hand, corporates such as PsiQuantum are embracing the concept of using quantum technologies to try and solve some of society's greatest challenges. The company recently set up Qlimate a "major quantum computing net zero initiative driving large-scale decarbonization". The organization is building partnerships with corporates, governments and non-profits to develop and scale end-to-end the most promising decarbonization solutions that will take years off the path to net zero. Other organizations have similar aims, for example Q4Climate and Entangle Climate (interview below).

Yet others in the industry have argued that presenting quantum technology as a solution to the climate crisis is little more than the next item in a long list of green-washing initiatives. Quantum computers are yet to produce useful commercial results at scale, let alone clear – in use – solutions to the climate crisis.

Detractors argue that we should be focusing on areas where we can make an impact now. We expect that this is a point of contention unlikely to go away until the community is able to demonstrate a tangible use case that has a positive impact on the environment.

Yet, this overlooks the significant number of quantum technology organizations (for example suppliers) who can consider their impact today, Oxford Instruments being an example.

OXFORD INSTRUMENTS INTERVIEW

Returning back to the documentary, we asked Stuart Woods, Managing Director at Oxford Instruments NanoScience, to reflect on the time since the making of our documentary.

TQI: What changes have you seen in the market?

SW: Unfortunately, with the current macroeconomic environment we have seen a greater stress on resources—particularly the availability of renewable energy. It almost feels like we have taken a step backwards. Even in the UK, with rising costs, we have seen a number of energy providers back away from renewable energy strategies. The situation has to change and we need to do more as regulation is not going to be enough to make a tangible enough impact . It looks very unlikely that we are going to be able to limit temperature increases to 1.5C by 2030, unless more businesses and governments prioritize investment in CO2 extraction, for example, putting our NetZero 2050 goal under threat.

TQI: How has your organization pushed its agenda forward?

SW: Within Oxford Instruments, we have made multiple positive advances. For the first time this year, we will have complete visibility of our full Scopes 1, 2, and 3 in line with GHG Protocols. We have also calculated our baseline year to understand, according to industry standard, SBTi, how much carbon we can offset. This gives us our first real data for calculating and making the hard decisions around moving to NetZero before 2050. The journey is just starting as this now brings into focus harder decisions, for example, around abatement activities. Carbon neutrality is not easy, but the first step is clear, industry standards-based monitoring and roadmapping to NetZero is a must. There is a lot of 'greenwashing' today which is why we must focus on best practices to achieve real results.

TQI: What are the next steps you want to see in the industry?

SW: I do believe that technology is a big part of the answer to slow climate change. Quantum computing should not be viewed as the new arms race. Climate change and the complex models of climate are a natural fit for quantum computing and for this reason alone we should look at global initiatives for climate change analysis using quantum computing. We are keen to support the industry in any initiatives and are keen to actively engage in programs to make a difference.

Having picked the brain of one expert on the theme of sustainability within the industry, we wanted to ask another individual's view.

ENTANGLE CLIMATE – A DISCUSSION WITH NICHOLAS LEE

Co-founder of Entangle Climate (along with Karan Pinto) — a non-profit whose aim is to accelerate innovation at the intersection of Quantum Computing and Climate Mitigation by aligning professionals across the ecosystem — Nicholas Lee is also Vice-head of Solution Innovation & Consulting AI/ML, Quantum-inspired and Decision Science at Fujitsu.

Lee says the avoidance of a climate disaster is the greatest challenge of the century. To make this happen, we need to transform the way we do almost everything. This beckons for breakthroughs and innovations that become new businesses and change existing ones. Today, it is almost free to pollute the atmosphere with CO2.

HARSH TRUTH

"The harsh meta truth: whether we like it or not, we need fossil fuel-based businesses for the solutions that accelerate our transition to decouple from CO2," says Lee.

Lee then shifted to capital markets and the fact they are aligned with sustainable development, seen as a keystone for helping to bridge the gap to combat Climate Change.

"The past decade has seen a surge in financial investments which are dedicated to sustainability. UNCTAD estimated in late 2020 that these new financial products and funding sources have invested $1.2-$1.3 trillion through areas such as clean energy, clean technology, sustainable agriculture, food

securities, sustainability-themed funds, green bonds, and social bonds, but with a sizeable gap remaining, and an annual reoccurring requirement, we must think outside the box for how we achieve this," says Lee.

"At the intersection of accelerating Climate Mitigation efforts is a significant role for quantum technologies as they have the means to reshape how we tackle and solve these social challenges. Quantum Computers are already showing significant advancements in many pressing areas such as accelerating drug discovery, enabling more efficient supply chains and providing more personalized healthcare services."

How do these problem characteristics transfer into the problems we need to address to tackle Climate Change?"

USE CASES

Lee believes the answer will come through initiatives like the open-ecosystem Entangle Climate, which he co-founded, one which is exploring over eighty use cases across six key pillars: Energy, Transport, Cities and Buildings, Agriculture, Industry, and Nature-based.

"Part of addressing this challenge is building an open awareness, unleashing knowledge from silos, and not trying to corner a particular market for the greater good of humanity. The other part, relative to quantum, is to embrace hybrid approaches that leverage a wide array of capabilities across simulation, emulation, gate-based systems, along with HPC, AI/ Machine Learning and Classical Solvers," says Lee, before adding a caveat:

"There is no silver bullet, no one compute will solve the entirety of the problems and we won't wake up one day and have all the answers. We must recognize the step changes we are making today with quantum computing and take a practical approach on how we find more efficient solutions for tomorrow."

INVESTING IN QUANTUM TO ADDRESS THE CLIMATE CRISIS

Another example of quantum addressing the problems of climate change is investment by impact / climate funds in the market. The Finnish startup IQM raised $128-million Series A2 funding round, led by World Fund, the largest European-focused climate venture capital fund that only invests in technologies with a Climate Performance Potential (CPP) of removing 100 million tonnes of carbon from the atmosphere annually by 2040 —something which IQM's quantum algorithms are apparently already busy tackling.

Daria Saharova, Founding Partner at World Fund, said of the investment: "Quantum computing holds the potential to drive the breakthroughs needed to help solve the climate crisis. We are proud to lead this round and support IQM's ambition to deliver quantum advantage to climate and sustainability goals.

8.Why it's time to take quantum-safe cryptography seriously

by IBM

https://research.ibm.com/blog/quantum-safe-cryptography-for-industry

Quantum-safe cryptography is here. It's time for industry to adopt it.

Quantum computers are maturing quickly — perhaps even quicker than we could have predicted five years ago. We see quantum technology's rapid pace of development in quantum technology as an important opportunity: We believe these machines are going to solve important problems in research and industry; that they're going to help us build a better world. But this rapid development also brings about an important consideration: The systems we use today to safeguard sensitive data will not be secure in a world where quantum computers have reached their full potential.

As we work to bring about quantum-centric supercomputing, we'll need to ensure that each facet of the computing workflow is prepared for this future. This means that private industry, government, healthcare providers, telco, and anyone else responsible for securing data or digital infrastructure will need to take steps today to make themselves quantum safe.

Already, the U.S. government is taking quantum-safe cryptography seriously: In May, the White House released a National Security Memorandum laying out the administration's plan for securing critical systems against potential quantum threats. Now the Department of Commerce's National Institute of Standards and Technology (NIST) has chosen four quantum-resistant tools that will be used as part of its "post-quantum cryptographic standard" — expected to be finalized in the next couple years. The four encryption methods were selected from a pool of 69 at the conclusion of a competition NIST announced in 2016.

IBM is proud to have developed three of these four tools in collaboration with our academic and industry partners. And today, IBM offers services to clients hoping to quantum-secure their data with IBM Quantum Safe.

Why quantum-safe matters

Today's cryptographic standards rely on problems that are easy for a computer to check but hard to solve. For example, classical computers can have a hard time figuring out the factors of large numbers — but it's easy to check that two prime numbers multiply together to some large numbers. So, modern encryption methods often use very large numbers as codes, such that their prime factors form the key. However, quantum algorithms offer solutions to some of these hard problems.

Back in 1994, mathematician Peter Shor developed an algorithm that could factor large prime numbers more quickly. That showed there was a way to crack these codes much more easily. Today's quan-

tum computers aren't yet capable of using Shor's Algorithm[1] to factor the numbers used in today's cryptosystems — but that will change as quantum computing systems mature in their scale, quality, and speed.

Already, governments are concerned that bad actors are positioning themselves to take advantage of next-generation code-breaking tools. Attackers could be stealing large tranches of encrypted data that would be unreadable using contemporary tools, hoarding data from these breaches with the intent to decode it once better technology becomes available. Organizations may have already experienced breaches that they will not know about for many years, creating an uncertain security and liability environment.

We don't know when it'll be possible to breach today's protocols — perhaps even in the next decade. However, the good news is that quantum-safe encryption, which relies on math problems that quantum computers also find difficult to solve, is already here. And it's crucial that we begin implementing these new protocols as soon as possible: Any data that falls into the wrong hands before an institution makes that transition should be considered already lost. Any computer systems that will have to operate securely without major modifications over a period of years — the computer in your next car, for example — will need to be quantum secure well in advance of the threat.

The time to prepare is now

Because of our expertise in both cryptography and quantum computing — and our key role in developing the new quantum safe standards — we are now working to prepare clients and partners for the transition to quantum-safe cryptography. We have also already incorporated NIST-approved quantum-safe algorithms into IBM's secure[2] hybrid cloud system z16

Upgrading the world's cybersecurity for the era of quantum computing will be a new challenge. Large institutions will need to transform their infrastructure with speed and agility. And still the task will take years, so it's crucial that anyone with critical data to secure — in other words, everyone — begins working on this right now.

Law and policy are still catching up with this new reality. Organizations that treat the NIST announcement as a watershed will be best positioned to protect their business interests and mitigate against liabilities.

IBM has developed a multi-step process toward rapidly making institutions quantum safe. We work with clients to identify where they are at vulnerable to quantum-based cryptography attacks. This is important: The risks vary substantially based on the type of applications and data an organization handles, as well as the state of its current cryptography. So the shift to quantum safe requires identifying the highest priorities for security.

---

[1] Watch the story of how Shor's algorithm came to be, as told by Peter Shor himself.

[2] Available on IBM z16: Future-Proof Digital Signatures with a Quantum-Safe Algorithm Selected by NIST.

Once priorities are set, we work with institutions to inventory their existing data and encryption schemes. Those inventories become frameworks for their transitions to quantum safe cryptography, enabling them to shift in a highly structured way first to a hybrid encryption scheme and then a fully quantum safe regime. Going through this process leaves their computing infrastructure more adaptable even after the transition. The next time a client needs to update their security, it can happen even faster thanks to the education and structure gained during this process.

We're already working with clients to identify their vulnerabilities, set goals, and create individualized roadmaps to prepare. This is a global challenge, but one that we have time right now to prepare for. Those preparations will leave us more resilient, more agile, and more able to adapt to future threats.

9.Quantum Computing Threat To Classical Symmetric Cryptography

by JAMES DARGAN

https://thequantuminsider.com/2022/07/26/quantum-computing-threat-to-classical-symmetric-cryptography/

Recently, Professor Guilu Long, Dr. Zeguo Wang, Dr. Shijie Wei from Tsinghua University and Beijing Academy of Quantum Information Sciences, and Professor Lajos Hanzo from the University of Southampton, UK, proposed a quantum attack scheme for symmetric cryptography, which may lead to a deadly threat to the security of symmetric cryptography such as AES.

So far, it is generally believed in the world that although quantum computers bring fatal threats to asymmetric cryptography such as RSA, they do not pose a fatal threat to symmetric cryptography such as AES. For symmetric cryptography such as AES, under Grover's attack, the computational complexity has changed from the n index of 2 (2^n) to the n/2 index of 2 ($2^{\frac{n}{2}}$), and the exponent complexity remains. Therefore, it is generally believed that as long as the key length is doubled, the corresponding security under a quantum computer can be achieved. At present, the upgrade and migration plan of the cryptosystem has been launched internationally.

The new attack method proposed by Professor Long Guilu and others uses Variational Quantum Algorithm (VQA). They studied the security of the symmetric cryptography S-DES (Simplified Data Encryption Standard) under the VQA attack. They constructed a Hamiltonian based on a pair of known plaintext and its corresponding ciphertext. The ground state of the Hamiltonian corresponds to the quantum state of the chosen ciphertext. By using variational methods, they found the ground state of Hamiltonian, then the key can be obtained. Simply put, in VQA, a quantum circuit is constructed in which there are several transformations with parameters, and these parameters are varied to obtain the minimum value of Hamiltonian. They used six ansatzes and two different classical optimization methods to calculate a total of 12 different variational strategies, and the results are shown in Table 2 of the article. Of the two optimization methods, the gradient descent method is better than the simplex method. The key can be obtained by 30–56 searches on average, which is similar to the 32

required by Grover's attack.

		N-M			GD		
		Maximum	Minimum	Average	Maximum	Minimum	Average
A	Y-Cx	694	28	449.40	94	2	55.27
	Y-Cy	693	38	454.03	94	3	65.67
	Y-Cz	692	21	385.83	94	2	39.50
B	Y-Cx	705	63	424.73	94	3	39.63
	Y-Cy	687	63	428.83	94	3	41.93
	Y-Cz	700	49	460.43	94	2	41.03

Y-Cx, Y-Cy, and Y-Cz represent the different ansatzes; N-M and GD represent the Nelder-Mead method and gradient descent method respectively; the figures represent the number of iterations. Source: ©Science China Press

Although the average number of iterations is similar to that of Grover's attack, the number of iterations of the variational method is not fixed. In some cases, the number of iterations is much lower than Grover's attack, even as low as 2. Figure 8 in the article shows the distribution of the number of iterations, corresponding to the strategy with gradient descent operation in the third row (A Y-Cz) of Table 2. For the same Hamiltonian and parameters, a total of 30 repeated simulations are performed, and if the simulations with more than 94 iterations have not converged, the simulation is stopped. The minimum number of iterations is 2 and the maximum number of searches is 94. When the number of iterations is between 2 and 5, there are ten times in total, accounting for one-third, which is a large proportion. In the actual calculation, the cutoff of the number of searches can be set lower, so that there is more time to try those variational schemes with a smaller number of searches.

The variational algorithm has no deterministic complexity, which is a disadvantage of it. However, in cryptanalysis, this complexity uncertainty turns into serious challenges to the security analysis of encryption cryptography such as AES, even the entire classical cryptographic algorithm based on computational complexity, under such attacks in quantum computing. Variational algorithms may bring more serious threats on these cryptographic algorithms than Shor's algorithm and Grover's algorithm. In particular, variational quantum algorithms are available on recent quantum computing hardware. If the results of this study hold in cryptographic algorithms with larger key size, such as AES-128, it will further strengthen this estimation and have a significant impact on the future course of information security.

It is worth noting that, in response to the threat of quantum computing to asymmetric cryptography such as RSA, classical cryptography has developed post-quantum cryptography. Recently the US National Institute of Standards and Technology announced the third-round winner. Analyzing the security of the post-quantum cryptography under variational quantum algorithms attacks is also a serious challenge.

Quantum technologies such as quantum secure direct communication and quantum key distribution can address this challenge. Quantum secure direct communication leaves the eavesdropper without any data related to the message, nothing to decipher, no matter how much computing power the decipherer has. Quantum key distribution makes it impossible for eavesdroppers to obtain any key information, and the use of these keys to encrypt the information with a one-time pad has been proved to be

undecipherable.

10.Researchers create key technology for quantum cryptography commercialization

by National Research Council of Science & Technology
https://techxplore.com/news/2022-07-key-technology-quantum-cryptography-commercialization.html

In modern cryptosystems, users generate public and private keys that guarantee security based on computational complexity and use them to encrypt and decrypt information. Recently however, modern public-key cryptosystems have faced potential security loopholes against quantum computers with great computational power. As a solution, quantum cryptosystems have been highly noticed. They use quantum keys that guarantee security based on quantum physics rather than computational complexity; thus, they are secure even against quantum computers. Therefore, quantum cryptosystems are expected to replace modern cryptosystems.

Quantum key distribution (QKD) is the most important technology for realizing quantum cryptosystems. Two main technical issues should be addressed to commercialize QKD. One is the communication distance, and the other is the expansion from one-to-one (1:1) communication to one-to-many (1:N) or many-to-many (N:N) network communication.

Twin-field (TF) QKD, announced in 2018, is a long-distance protocol, which can dramatically increase the communication distance of QKD systems. In TF QKD, two users can distribute a key by transmitting quantum signals to an intermediate third-party that is for measurement. Given the inevitable channel loss, this architecture allows the users to increase the communication distance. However, despite its innovativeness, it has been experimentally demonstrated by only a few global QKD leading groups owing to the significant difficulty of system implementation, and research on the TF QKD network is still insufficient.

The Korea Institute of Science and Technology (KIST, Director Seok-jin Yoon) announced that their research team, the Center for Quantum Information, led by director Sang-Wook Han, succeeded in an experimental demonstration of a practical TF QKD network. This is the second experimental demonstration of the TF QKD network in the world after the University of Toronto in Canada.

In their study published in npj Quantum Information, the research team proposed a new TF QKD network structure scalable to a two-to-many (2:N) network based on polarization-, time-, and wavelength-division multiplexing. Unlike the first demonstration of the University of Toronto based on a ring network structure, the research team's architecture is based on a star network. The quantum signal in a ring structure must pass through every user connected to the ring, however, the star structure only has it go through the center, making it possible to implement a more practical QKD system.

Besides, to overcome the main implementation obstacles to developing the TF QKD system, the team applied a plug-and-play (PnP) structure. A conventional TF QKD system requires many control systems,

such as timing, wavelength, phase, and polarization controllers, to maintain the indistinguishability of two quantum signals emitted by two users' different light sources. Whereas in the PnP TF QKD architecture developed by the KIST research team, the middle third-party generates and transmits the initial signals to both users using a single light source, and the signals return to the third-party by making a round trip. Therefore, the polarization drift due to the birefringence effect of the channel is automatically compensated, and users have fundamentally the same wavelength. In addition, due to the two signals passing through the same route in opposite directions, the arrival times of the signals are naturally identical. As a result, only a phase controller is required for implementing the research team's architecture. Based on the architecture, the team successfully conducted an experimental demonstration of a TF QKD network.

"It is a significant research achievement showing the possibility of solving the two main obstacles to QKD commercialization, and we have gained a key technology leading the corresponding research," said Sang-Wook Han, the leader of the Center for Quantum Information.

11.Towards a broader use of Quantum Key Distribution in telecommunication network

by Patrick Shore

https://www.idquantique.com/towards-a-broader-use-of-quantum-key-distribution-in-telecommunication-network/?utm_term=Towards%20a%20broader%20use%20of%20Quantum%20Key%20Distribution%20in%20telecommunication%20network&utm_campaign=Quantum%20Era%20Security%20Times%20July%202022&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%20July%202022-_-Towards%20a%20broader%20use%20of%20Quantum%20Key%20Distribution%20in%20telecommunication%20network

Last week, the ITU-T[3] adopted two new work items regarding the control and interworking of quantum key distribution (QKD) networks. Acting as editor, our partner SK Telecom coordinated and facilitated their development.

1. 'Software Defined Networking Control System for Interworking of Quantum Key Distribution Networks' allows telecommunication companies to manage their existing communication networks and QKD networks in an integrated and efficient manner. It also enables the integrated management of quantum cryptography communication networks- using QKD of different equipment vendors, a huge boost to the growth of the related ecosystem as telecommunication companies will be able to work with multiple equipment vendors to deploy quantum-powered networks.

[3] International Telecommunication Union refers to the field of telecommunication standardization, and Affiliated organizations set standards in the field of communication

2. 'Quantum Key Distribution Network Federation' can be compared to international roaming between mobile operators. Just like international roaming provides users with mobile services beyond national boundaries, 'Quantum Key Distribution Network Federation' allows the provision of quantum-safe communication services regardless of whose QKD network users are on by supporting interworking/federation between QKD networks of different service providers.

These two work items will be approved as international standards through further discussions among ITU-T member countries, with the aim of easing the adoption of quantum key distribution in telecommunication networks globally.

ID Quantique and SK Telecom move one step forward in their standardization roadmap for quantum key distribution

IDQ and SK Telecom have been working closely to promote international standardization of quantum-safe technologies including QKD and QRNG, while expanding the quantum technology ecosystem and market. Their joint standardization roadmap aims at a wider deployment and implementation of QKD networks. This new step is contributing to a faster and wider adoption of quantum-based cybersecurity. Standards play a central role in building trust, as the agreement of industry standards is a sign of the maturity of a technology and its supporting ecosystem.

12.The Race to Ensure Post Quantum Data Security

by John Russell
https://www.hpcwire.com/2022/07/21/the-race-to-ensure-post-quantum-data-security/

Fault-tolerant quantum computers won't exist for years – a decade is the most common estimate. When they do arrive, thanks to Shor's now-famous algorithm, they will be able to crack the most widely-used encryption methods, which are based on factoring. Earlier this month, the National Institute of Standards and Technology (NIST) settled on four algorithms – one for public-key-encryption (KEM) and three for digital signatures – based on lattice problems and hash functions, for incorporation into new post-quantum encryption standards.

These are deliverables of NIST's post-quantum cryptography standardization project (PQC), begun in 2016 and involving multiple rounds of submissions by industry, academia, and public entities, and assessment by NIST. This was the third round. A final fourth round is planned to consider four more algorithms.

NIST has issued a thorough report detailing the PQC process and sharing, for example, benchmark data across multiple processor types, and explaining NIST's rationale for the selections. Three selection criteria were used:
1) security (most important),

2) cost and performance, and
3) algorithm and implementation characteristics.

The latest NIST report isn't news in the sense that the quantum community and virtually all enterprise data security professionals have been closely tracking NIST's PQC efforts.

Table 4. Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS-Kyber	CRYSTALS-Dilithium
	Falcon
	SPHINCS+

Table 5. Candidates advancing to the Fourth Round

Public-Key Encryption/KEMs	Digital Signatures
BIKE	
Classic McEliece	
HQC	
SIKE	

Even as NIST works to formalizes the new standards, it has begun a new project – Migration to Post Quantum Cryptography – in collaboration with industry to develop tools and migration practices to protect data. That project is being run by NIST's National Cybersecurity Center of Excellence (NCCoE). Here's a snapshot of the program's main goals:

- Demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes.

- Once the public-key cryptography components and associated assets in the enterprise are identified, the next project element is prioritizing those applications that need to be considered first in migration planning.

- Finally, the project will describe systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across different types of organizations, assets, and supporting technologies.

NIST issued a Cooperative Research and Development Agreement (CRADA) to work on the project and last week disclosed the list of vendors who've signed on to participate so far: Amazon Web Services, Inc. (AWS), Cisco Systems, Inc., Crypto4A Technologies, Inc., Cryptosense SA, InfoSec Global, ISARA Corporation, Microsoft, Samsung SDS Co., Ltd., SandboxAQ, Thales DIS CPL USA, Inc., and Thales Trusted Cyber Technologies, VMware, Inc.

Bottom line: The race to develop tools to protect data from quantum computer-based attacks has begun in earnest.

It's been reported that more than 20 billion devices will need to upgrade their software to PQC before quantum computers crack RSA encryption. "Adversaries are already engaged in Store Now Decrypt Later (SNDL) attacks — stealing and storing encrypted data (e.g., financial records, intellectual property, medical records, etc.) to crack and exploit later when quantum computers become readily available," says Google spinout, SandBoxAQ, a CRADA participant.

The first step, of course, was selection of the first set of PQC algorithms, intended for use in public-key encryption (KEMs) and digital signatures. HPCwire recently talked with Vadim Lyubashevsky, a prominent cryptography analyst and IBM researcher whose contributions have been important for the NIST PQC. Lyubashevsky provided insight into development and characteristics of effective encryption.

The history of cryptography is fascinating. It blends political and industrial intrigue and clever mathematics, and has affected the outcomes of war. The enigma machine for decoding German communications during World War II is perhaps the most dramatic modern example. Cryptography features an exotic vocabulary – one-way functions, computational hardness, average case and worst case hardness, NP-completeness, supersingular isogeny key exchange, and lattice problems – that is opaque to most except cryptographers and mathematicians. Yet securing data and communications is fundamental to so many areas of life.

Interestingly, most modern encryption schemes begin as problems that mathematicians can't solve with current RSA factoring-based encryption as an example.

Lyubashevsky said, "The way we gauge [cryptographic] strength is by having people try to solve the underlying mathematical problem. If the community dedicates a lot of effort to it for a few decades and it's not successful, then we think that it's secure, the underlying mathematical problem. Then we build cryptography, based on that problem. It's the reason we think that factoring is secure against [attack from] classical computers; people have been trying to solve factoring for over 40-50 years and haven't been successful so we think it's okay."

"The problems that they originally came up with in the 1970s, these factoring discrete logarithms and all the things about elliptic curves. They stayed classically hard. Of course, better algorithms for factoring appeared but in some sense, there wasn't some catastrophic break and all of a sudden, somebody just broke it. But now, when a quantum [fault tolerant] computer exists, it will be completely broken."

"The same thing with lattice algorithms. People have been trying for a shorter amount of time, let's say seriously trying for 20-25 years, to break these underlying mathematical problems," he said. So far, no game-changing algorithm for solving lattice problems on a quantum computer has arisen.

The lattice problem, upon which three of the NIST PQC selected algorithms are based, is commonly illustrated as The Knapsack Problem and dates back to the late 1890s. This description is from Wikipedia: "Given a set of items, each with a weight and a value, determine the number of each item to include in a collection so that the total weight is less than or equal to a given limit and the total value is as large as possible. It derives its name from the problem faced by someone who is constrained by a fixed-size knapsack and must fill it with the most valuable items. The problem often arises in resource allocation where the decision-makers have to choose from a set of non-divisible projects or tasks under a fixed budget or time constraint, respectively."

IBM Research has even published a short video describing the knapsack problem and its relevance to quantum cryptography.

Lattice reduction algorithms can be used to tackle the problem but the computational resources re-

quired are impractical. Wikipedia, once again: "The conjectured intractability of such problems is central to the construction of secure lattice-based cryptosystems: Lattice problems are an example of NP-hard problems which have been shown to be average-case hard, providing a test case for the security of cryptographic algorithms. In addition, some lattice problems which are worst-case hard can be used as a basis for extremely secure cryptographic schemes. The use of worst-case hardness in such schemes makes them among the very few schemes that are very likely secure even against quantum computers."

Likewise, hash function cryptography also has a lengthy history. These functions are said to be one-way functions, which means it is practically infeasible to invert or reverse the computation. Ideally, the only way to find a message that produces a given hash is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes.

Lyubashevsky points out that work on these difficult mathematical problems often starts out seeking solutions for useful applications.

"These are natural mathematical problems. If somebody does find a fast algorithm for them, it will have positive effect in the areas of optimization and things like that," he said. "So these are questions people are interested in solving positively. But since they couldn't, you know, we base cryptography on it. As far as quantum computing goes, it's kind of the same story. People who specialize in quantum algorithms know these lattice problems. A lot of these lattice cryptography problems originated from people working in quantum algorithms trying to find a new type of algorithms that a quantum computer can solve and they didn't succeed."

In its PQC program, NIST asked for security equivalence of AES-128 and AES-192 (AES, advanced encryption standards) against quantum computers. The 128 and 192 refer to the bit size of keys. There is also an AES-256 but that was not requested.

The PQC program included five security strength categories "based on the computational resources required to perform certain brute-force attacks against the existing NIST standards for AES and SHA in a variety of different models of the cost of computation, both classical and quantum…The idea is that in order to meet, for example, category 1, the best attack violating the security definition of a parameter set should cost more than a brute-force key search attack on a single instance of AES-128, according to any plausible assumption regarding the relative cost of the various computational resources involved in a real-world attack.[i]" (A list of the five security strengths is included at the end of the article.)

As acknowledged by NIST, there's room for some disagreement about what constitutes relative computational cost – "including quantum gates, classical gates, quantum memory, classical memory, hardware, energy, and time" – and how much of a given resource an attack actually requires."

Talking about the submissions to NIST, Lyubashevsky said, "We had to provide them the parameters for which we believe these (AES) problems are secure at these levels. Now, of course, it's a bit messy. Things do change a bit even during the standardization effort. There were attacks that lowered security by, you know, five bits or 10 bits. This does require us to increase parameters."

This type of ongoing change has happened with factoring schemes, said Lyubashevsky, "because the original things that were proposed in or 1970s can be broken on a cell phone now, and not just because better technology exists, but because better algorithms have been developed."

Focusing on the NIST PQC effort, "All these algorithms kind of existed before in this [NIST PQC] competition with lattice algorithms. The main positive effect of the standardization effort is that it got a lot more cryptanalysts looking at these problems. I think most cryptanalysts work for government agencies like the NSA, GCHQ, and places like that," said Lyubashevsky.

Given all the scrutiny, Lyubashevsky thinks we can be confident about the security of the PQC algorithms selected. Moreover, he thinks advancing computational hardware technology isn't a big threat.

"Cryptography should not be affected by any of this (advancing supercomputers), because we believe the hardness of the problem (lattice) is exponential. If you increase your computing power by a factor of two, you just increase the key by one bit, I mean there is a limit to how much computing can increase; you cannot probably do more operations beyond some energy threshold." There's only so much energy available on the planet, he wryly chides, "the security of the cryptography kind of goes above this threshold, and it's not hard to get it above it," he said.

The lattice algorithms used for public-key encryption are faster and smaller than hash function algorithms, according to Lyubashevsky.

"You can't get public key encryption from hash functions; you can only get digital signatures. It's slower and bigger but one big advantage is that the security of hash functions, are not really based on any mathematical problem, it's just random stuff and should be hard to invert. People will be very, very surprised if something like SHA-3 (secure hash algorithm-3) falls to quantum computing," he said. "This would be a complete shock and a lot of symmetric key cryptography would be broken. This is not something that we're even discussing in terms of this NIST standardization effort," he said.

NIST intends to select at least one more KEM for standardization after the fourth final round of assessments. Lyubashevsky notes there are always tradeoffs between encryption schemes and implementations of the same scheme. For example the submitted algorithms may vary in size, may require different amounts of computational resources, have have different performance characteristics.

"Maybe with respect to some new candidates that's something NIST will consider in round four. For example, there's this other type of mathematics based on supersingular isogeny math. It provides solutions smaller than lattices, but it's very, very slow. So that's something they may want to standardize in the fourth round. They want different digital signatures [and] there you also have a lot of tradeoffs. Something can have a much smaller signature but a much larger public key. The lattice-based scheme is very balanced, whereas other kinds of specialist schemes can have an advantage in one area and a big disadvantage from another," he said.

Despite the work still to be done, NIST wants industry and the encryption community to push ahead and not wait. "Even though the third round is ending and NIST will begin to draft the first PQC standards, standardization efforts in this area will continue for some time. This should not be interpreted to mean that users should wait to adopt post-quantum algorithms. NIST hopes for rapid adoption of

these first standardized algorithms," is the guidance from the just-released report.

Lyubashevsky says the need to revamp security has highlighted the ad hoc way in which encryption has often been applied and spotlights the need for a more orderly approach going forward.

"I was a bit surprised when the folks at IBM who actually work on this stuff [deployment and products] said finding the cryptography in data is hard because the crypto is intermingled with everything else, with all the other code and the all the other programs. It's hard to find and [therefore] hard to yank out and put something else in. This was all an artifact from the 80s and 90s," he said.

What's needed now, said Lyubashevsky, is a more modular approach. "If we're going to change everything, let's at least do it right. Let's make everything modular so if something needs to be changed in the future, for whatever reason, it's easy to take out and plug in something new. This is also important in quantum safe cryptography because you don't have an algorithm that is best at everything; you have some that are very fast, you have some that are very slow, but have slightly smaller keys. There will be scenarios where one is better than the other. And maybe you don't quite know which one it will be and you want to be agile. You want to be able to quickly put algorithms in and take algorithms out."

Link to latest NIST report
Link to NIST migration project
Strength Categories from NIST

1) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES-128)
2) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA-256/ SHA3-256)
3) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES-192)
4) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA-384/ SHA3-384)
5) Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g. AES-256)
6) Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, https://csrc.nist.gov/publications/detail/nistir/8413/final

13.How the NSA Is Moving Toward a Quantum-Resilient Future

by Patrick Shore
https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-nsa-moving-toward-quantum

Quantum computing is a rapidly advancing technology that has the potential to transform industries by solving complex optimization problems that elude classical computers. But what happens when a quantum computer is used against the digital infrastructure that safeguards our nation's most sensitive data? This is a question that the National Security Administration (NSA) is not waiting to find out, and neither should private organizations.

Quantum computers utilize the quantum properties of subatomic particles to perform countless calculations simultaneously and, in a matter of seconds, solve problems that even today's most powerful supercomputers would take thousands of years to complete. Consider the uses for such a computer in optimizing financial investment portfolios, vehicle routing, manufacturing processes, energy resource allocation, and drug development, and the transformational potential of quantum computing becomes clear. However, the rapid development of these revolutionary supercomputers has caused alarm in the defense sector as adversarial nation-states are currently investing billions of dollars to weaponize quantum computers.

The Department of the Defense's (DoD) primary concern is that a weaponized quantum computer could be used to break the encryption that protects sensitive government data and communications. There are thousands of scientists, mathematicians, and quantum programmers currently employed by adversarial nations to advance the quantum threat against the United States. A quantum computer that could disrupt vital digital systems and decrypt classified information presents an enormous national security threat. The United States has responded by developing technologies to counter the quantum threat and reinforce its digital infrastructure. In particular, the NSA has been tasked with ensuring the future security of the United States' digital infrastructure by implementing quantum-resilient solutions on national security systems (NSS).

The NSA Recognizes the Quantum Threat

In 2015 the NSA announced a plan to transition NSS to a new quantum-resilient cipher suite. Though quantum computers were still in their embryonic state, the NSA explained that the threat of quantum computing was the primary consideration in the decision to withdraw the previous cipher suite, called Suite B, and prepare for the post-quantum era. The NSA stated in their announcement, "Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, necessitating a re-evaluation of our cryptographic strategy." The announcement also noted that the ultimate goal for the agency was to "provide cost-effective security against a potential quantum computer."

This announcement was the first time that the NSA publicly recognized that quantum computing posed a serious threat to encryption and, more importantly, that it was time to act. It's also important to note that the NSA seeks a cost-effective solution. This will undoubtedly be a key obstacle for organizations across the government and private sectors during the transition to Post-Quantum Cryp-

tography (PQC). For a solution to be cost-effective it must be compatible with existing systems; replacing hardware presents significant challenges and expenses. The NSA has deferred to the National Institute of Standards Technology (NIST) to research PQC solutions and finalize a set of quantum-resilient algorithms for use in NSS. The cost-effectiveness of this approach will largely depend on each organization's ability to implement the new algorithms with minimal disruption to existing systems.

What the NSA is Not Doing

The NSA has explored many options for quantum-resilient solutions, including Quantum Key Distribution (QKD). QKD primarily uses photonic channels (fiber optics) to send unique encryption keys generated through the quantum properties of photons. While keys used in QKD are strong, the technology is vulnerable to weak implementation which causes it to be susceptible to a variety of quantum and even classical attacks.

Aside from the security vulnerabilities, another fundamental issue plaguing QKD is the amount of specialized hardware required to secure a connection between two points. The NSA has stated that implementing QKD on NSS would require significant resourcing, and it did not qualify as a comprehensive quantum security solution. According to the NSA, QKD "only addresses some security threats and it requires significant engineering modifications to NSS communications systems. NSA does not consider QKD a practical security solution for protecting national security information." The complexity of QKD undermines the goal of the NSA to provide cost-effective quantum cybersecurity as stated in the 2015 announcement. The NSA and NIST have both endorsed PQC as the superior and cost-effective quantum-resilient solution and, ultimately, PQC will become the standard for data encryption in both the government and private sectors.

Expediting the NSA's Efforts

The timeline for the NSA's effort to transition to PQC was shortened significantly when in January President Biden signed a National Security Memorandum (NSM-8) on "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems." The memo specifically called upon the NSA and the Committee for National Security Systems (CNSS) to, within 180 days, identify instances of encryption used on NSS not in compliance with NSA-approved quantum-resistant algorithms, as well as to provide a plan and timeline to transition those systems to quantum-resistant standards.

The NSA can no longer wait until 2024 for NIST to finalize PQC standards and is now tasked with auditing the current NSS cyber infrastructure and providing a PQC transition plan immediately. This mandate marked the beginning of the biggest upcycle in cybersecurity history for the DoD. Private organizations would be wise to act with the same urgency as the NSA and begin exploring post-quantum solutions for their own systems.

Interagency Collaboration

A successful transition of the NSS to PQC will require the collaboration of multiple government authorities. Section 1(v) of NSM-8 requires the NSA to collaborate with the Department of Homeland

Security (DHS) and other national security organizations on coordinating this transition process. Recently, the DHS released a roadmap outlining a step-by-step PQC transition strategy for government and commercial agencies to take inventory of their most sensitive information and prioritize the upgrade of their systems accordingly. This will be a useful tool for the NSA as the agency conducts a similar evaluation process for NSS. The DHS tool is open to the public and offers a valuable resource for private organizations to conduct similar audits on their own systems.

The Need for Public-Private Collaboration

The NSA has consistently held its door open for collaboration with the private sector which will be critical as the United States moves forward into a new generation of cybersecurity. The NSA's Commercial Solutions for Classified (CSfC) Program is a platform that allows private commercial developers (i.e., vendors) to register cybersecurity components of Commercial Off The Shelf (COTS) products for use on NSS. These components are compiled into vendor-agnostic Capability Packages (CP) that are provided to CSfC clients, including DoD, intelligence communities, military services, federal agencies, and other NSS stakeholders. While the CSfC will not field commercial solutions for post-quantum algorithms until NIST completes its PQC standards research and recommendations, there are many resources available through CSfC designed to help clients, which include both government and private organizations using NSS, ease the upgrade process.

The National Cyber Center of Excellence (NCCoE) has launched a Post-Quantum Migration Project that brings together academic, industry, and government experts to develop a set of tools for organizations to audit their systems, assess risk, and prepare for the quantum upgrade. This type of public-private collaboration will be critical to ensuring that both the government and private sectors navigate the transition smoothly. The private sector must follow the lead of the NSA and other cyber authorities and begin preparing their systems for the transition to PQC to ensure that the digital infrastructure that supports the United States remains secure now, and into the quantum era.

14.SK Telecom to Lead International Standardization of Quantum Cryptography Technologies

by Ray Sharma
https://www.thefastmode.com/technology-solutions/26331-sk-telecom-to-lead-international-standardization-of-quantum-cryptography-technologies

SK Telecom announced that its two technologies regarding the control and interworking of quantum cryptography communication networks were adopted as new work items at the ITU-T meeting held in Geneva, Switzerland. They will be approved as international standards through discussions among ITU-T member countries.

The two technologies chosen as work items are: 'Quantum Key Distribution Network Interworking – Software Defined Networking Control'; and 'Framework of Quantum Key Distribution Network Federation.' Both of these technologies are essential for the popularization of quantum cryptography communication technologies.

'Software Defined Networking Control System for Interworking of Quantum Key Distribution Networks' allows telecommunication companies to manage their existing communication networks and QKD networks in an integrated and efficient manner.

It also enables integrated management of quantum cryptography communication networks using QKD of different equipment companies, which will be a huge boost to the growth of the related ecosystem as telecommunication companies will be able to work with multiple QKD equipment companies to deploy quantum-powered networks.

'Quantum Key Distribution Network Federation' can be likened to international roaming between mobile operators. Just like international roaming provides users with mobile services beyond national boundaries, 'Quantum Key Distribution Network Federation' allows for the provision of quantum-safe communication services for customers regardless of whose QKD network they are on by supporting interworking/federation between QKD networks of different service providers.

Going forward, this technology is expected to not only enable the federation of QKD-equipped national backbone network and QKD networks of telecommunication companies to support joint roaming services in emergencies, but also allow for the federation of satellite communication networks and QKD networks to offer a new range of quantum cryptography communication services in the era of 6G mobile communication.

Meanwhile, together with the SK Broadband consortium and ID Quantique, SKT has implemented projects for the Ministry of Science and ICT, building pilot QKD infrastructure and developing application services for 17 different institutions from the public, medical and industrial sectors. In addition, the company is currently working to expand into the defense and public markets in cooperation with competitive Korean cryptography companies.

15.Israel to establish quantum computing R&D center, build quantum computer

by RICKY BEN-DAVID

https://www.timesofisrael.com/israel-to-establish-quantum-computing-rd-center-build-quantum-computer/

Israel is moving ahead with plans to lay the foundation for quantum computational ability, which it has said would lead to future developments in economics, technology, security, engineering, and science.

This week, the Israel Innovation Authority announced a budget of NIS 100 million ($29 million) to

build a quantum computing research center, headed by Israeli startup Quantum Machines, which will also help build a quantum computer.

Quantum Machines, founded in 2018, has built a hardware and software solution — Quantum Orchestration Platform (QOP) — for operating quantum systems to facilitate research and enable future breakthroughs. It also developed the QUA, a standard universal language for quantum computers that the startup says will allow researchers and scientists to write programs for varied quantum computers with one unified code.

The company already provides quantum computing services to customers in over a dozen countries, including multinational corporations, government laboratories, academic institutions, and quantum development startups. Quantum Machines recently announced a partnership with Toyota Tsusho Corporation, the trading arm of automotive giant Toyota, to build future quantum capabilities and offer the multinational's Japanese customers access to quantum technologies.

Israel's new quantum computing center is part of the NIS 1.25 billion ($390 million) Israel National Quantum Initiative, launched in 2018 to facilitate relevant quantum research, develop human capital in the field, encourage industrial projects, and invite international cooperation on R&D.

In February, the Israel Innovation Authority and the Defense Ministry announced that they planned to spend approximately NIS 200 million ($62 million) to develop a state quantum computer and lay the foundation for Israeli computational ability in the field. The NIS 100 million budget is part of this plan.

The Defense Ministry's Directorate of Defense Research and Development (DDR&D) will issue a separate tender to finance the development of quantum technologies for military use for another NIS 100 million, the innovation authority said.

Quantum Machines, together with a consortium of Israeli and international quantum tech companies at the center, will build a quantum computer to be made available to the commercial and research communities.

The center will offer access to research and development on three quantum processing technologies — superconducting qubits, cold ions, and optic computes — and provide services to the Israeli quantum computing community, the Israel Innovation Authority said Sunday.

Itamar Sivan, co-founder and CEO of Quantum Machines, said in a company statement the goal of the project was "to give Israeli companies access to the most advanced quantum technologies and services so that they can develop deep quantum expertise across industry and academia. This expertise will allow Israeli companies across a broad range of sectors and industries to gain a leading global position."

Ami Appelbaum, chairman of the Israel Innovation Authority, said the new center was "the answer to an existing strategic market failure and is part of the authority's policy of enabling the industry to maintain its leading position at the forefront of breakthrough and disruptive technologies."

Countries like China, Japan, the US, Germany, and India are also pouring millions into developing their own quantum abilities.

According to recent market projections, the global quantum computing market size is expected to grow from about $470 million in 2021 to about $1.765 billion by 2026.

Quantum computing is a relatively new and extremely complex field, but experts say that the abilities can be extremely beneficial in industries like cybersecurity, materials and pharmaceuticals, banking and finance, and advanced manufacturing, and may lead to massive developments in broad fields like economics, security, engineering, and science.

In a nutshell, quantum computing harnesses quantum mechanics to quickly solve problems that are too complex for classical computers. Quantum computers process exponentially more data compared to classical computers, using quantum bits, or qubits, the basic unit of quantum information.

16.Our new Quantum Virtual Machine will accelerate research and help people learn quantum computing

by Catherine Vollgraff Heidweiller
https://blog.google/technology/research/our-new-quantum-virtual-machine-will-accelerate-research-and-help-people-learn-quantum-computing/

Several decades ago, quantum computers were only a concept — a distant idea discussed mostly in lecture halls. Flash forward to today, and the race is on to build fault-tolerant quantum computers and discover new algorithms to apply them in useful ways.

For all the aspirations of quantum computing, the reality is that unlocking its potential to solve real-world problems is as challenging as building the quantum computers themselves. This got us thinking... how can we empower more people to join us on the quest to discover quantum algorithms and applications? Can we make prototyping quantum algorithms for near term quantum computers free of cost and easy to get started with so that people can focus on the challenge at hand? Can we provide people with the tools they need to equip themselves with the quantum programming skills required for application development?

At Google Quantum AI, we have a long history of making tools we build for our own research available to the public free of cost. Today we are adding the Quantum Virtual Machine to the list. The Quantum Virtual Machine (QVM) emulates the experience and results of programming one of the quantum computers in our lab, from circuit validation to processor infidelity. We feed measurements from our Sycamore processors, such as qubit decay, dephasing, gate and readout errors into the QVM and combine these with the qubit connectivity of the device to simulate quantum processor-like out-

put, using our physics research team's models. You can see comparisons between results obtained from experiments on a Sycamore chip and the QVM on this site.

The Quantum Virtual Machine can be deployed instantly from a Colab notebook and is available free of cost. You do not have to wait in a queue to get your program's results and can iterate on results quickly. This, combined with processor-like output makes the QVM a great tool for prototyping, testing and optimizing your quantum circuit for near term quantum hardware. Users can currently emulate two of our processors: Weber and Rainbow. Weber is the Sycamore processor that was used in our beyond-classical experiments published in Nature in 2019. Rainbow was used in our experiments demonstrating the variational quantum eigensolver on quantum chemistry problems published in Science.

Once you have deployed your Quantum Virtual Machine, you can run your quantum program on a grid of virtual qubits. If you require more qubits than can be simulated through Colab, the QVM can be supercharged with additional high-performance compute of your choice. This workflow helps you set up a simulation on multiple parallel compute nodes with Google Cloud. To build your quantum program, you can use Cirq 1.0, the newly released version of our open-source quantum programming framework.

We hope that you will find the Quantum Virtual Machine useful while exploring quantum computing, whether for research or education. For educators and their students, the QVM makes it possible to complete coursework and projects on a top quality processor, without running into the long and unpredictable queues that are common in the industry. We have also created supporting documentation that exposes several of the features of the QVM and Cirq 1.0 to enable students to onboard quickly.

With every major improvement in quantum hardware, the need to discover useful applications and to develop the global quantum workforce of the future grows. Join us on our quest to push the boundaries of innovation in quantum algorithms using the Quantum Virtual Machine. Get started at quantumai.google/software.

17.Toshiba, Safe Quantum Enter Agreement to Accelerate Quantum Communication Solutions in North America

by James Dargan

https://thequantuminsider.com/2022/07/15/toshiba-safe-quantum-enter-agreement-to-accelerate-quantum-communication-solutions-in-north-america/?utm_source=newsletter&utm_medium=email&utm_term=2022-07-22&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+NVIDIA+s+Quantum+Platform+Q2+sWild+Waves+--+And+More+Quantum+News

Toshiba recently announced a partnership with Safe Quantum in the areas of quantum key distribu-

tion (QKD) and quantum communications. Led by John Prisco, Safe Quantum champions the commercial adoption of quantum technology and will support Toshiba's ongoing work to secure the quantum future.

Data breaches and security incidents across all industries are on the rise, and with heightened concerns about serious cybersecurity threats, governments and businesses are recognizing the critical need for new ways to effectively manage sensitive data and protect vulnerable infrastructures against cyberattacks. Unlike conventional encryption, QKD solutions use encoded photons to secure the distribution of encryption key material that is unhackable—a major driver in why North America is expected to account for the largest share of the global Quantum Cryptography market. The collaboration will help fulfill the increasing interest among potential users in North America looking to better understand QKD solutions as a new system to safeguard their communications against future threats.

"We're proud to partner with Safe Quantum in our shared vision of keeping the transmission of sensitive information safe and secure through our reliable and ultra-secure quantum cryptography solutions," said Tsuyoshi Sasano, who is vice president of digital solutions and leads Toshiba's QKD business in North America. "This collaboration furthers Toshiba's global expansion of our QKD business in North America, with previously established partnerships in Japan and the UK."

Toshiba started research into quantum cryptography in 2003. Since then, it has demonstrated several notable world firsts, including being the first to announce QKD over 100km of fiber in 2004. This means its fiber-QKD platform products are able to address quantum-secure communication requirements over hundreds of kilometers in metropolitan areas. Toshiba was also the first with a continuous key rate exceeding 1 Mbit/second in 2010 and 10 Mbit/second in 2017. And in 2020, it set the new world's fastest record for any QKD system to date of 13.7 Mb/s over 10km of fiber. In February, they announced the first successful proof-of-concept test to secure mission-critical blockchain applications with QKD alongside JP Morgan Chase and Ciena.

"2022 will mark the year we see commercial quantum technology really take off, as more innovators see the future quantum-secure world as the ultimate way to protect data," said John Prisco, CEO and founder of Safe Quantum. "We are delighted to be partnering with Toshiba on this important use case for quantum information science."

18.VISUAL CRYPTOGRAPHY FOR PHYSICAL KEYRINGS

by Dave Rowntree
https://hackaday.com/2022/07/14/visual-cryptography-for-physical-keyrings/

Visual cryptography is one of those unusual cases that kind of looks like a good idea, but it turns out is fraught with problems. The idea is straightforward enough — an image to encrypt is sampled and a series of sub-pixel patterns are produced which are distributed to multiple separate images. When individual images are printed to transparent film, and all films in the set are brought into alignment,

an image appears out of the randomness. Without at least a minimum number of such images, the original image cannot be resolved. Well, sort of. [anfractuosity] wanted to play with the concept of visual cryptography in a slightly different medium, that of a set of metal plates, shaped as a set of keyrings.

Metal blanks were laser cut, with the image being formed by transmitted light through coincident holes in both plate pairs, when correctly aligned. What, we hear you ask, is the problem with this cryptography technique? Well, one issue is that of faking messages. It is possible for a malicious third party, given either one of the keys in a pair, to construct a matching key composing an entirely different message, and then substitute this for the second key, duping both original parties. Obviously this would need both parties to be physically compromised, but neither would necessarily notice the substitution, if neither party knew the originally encrypted message. For those interested in digging in a little deeper, do checkout this classic paper by Naor and Shamir of the Wiezmann Institute. Still, despite the issues, for a visual hack it's still a pretty fun technique!

19.Mantis botnet behind the record-breaking DDoS attack in June

by Bill Toulas

https://www.bleepingcomputer.com/news/security/mantis-botnet-behind-the-record-breaking-ddos-attack-in-june/

The record-breaking distributed denial-of-service (DDoS) attack that Cloudflare mitigated last month originated from a new botnet called Mantis, which is currently described as "the most powerful botnet to date."

The attack peaked at 26 million requests per second that came from 5,067 devices. The previous record was held by Mēris botnet, which launched an attack that spiked at 21.8 million requests per second.

DDoS mitigation company Cloudflare, has been tracking Mantis botnet attacks against one thousands of its customers.

Not your ordinary botnet

Cloudflare explains in a report today that its analysts named the botnet Mantis after the Mantis Shrimp that can deliver devastating blows with its claws while being roughly 10 cm (4 inches) long. Similarly, the botnet is extremely powerful despite relying on a small number of devices.

Typical botnets need to compromise a large number of connected devices to accumulate sufficient firepower to deliver disrupting attacks against protected targets.

Mantis targets focuses on servers and virtual machines, which come with significantly more resources.

Generating many HTTPS requests is a resource-demanding process, so the more powerful the devices that constitute the botnet swarm, the more potent the DDoS attacks they can launch.

The previous record holder, Mēris, achieved particularly strong attacks by recruiting MikroTik devices, which feature powerful hardware.

Mantis victims

Mantis targets entities in the IT and telecom (36%), news, media, and publications (15%), finance (10%), and gaming (12%) sectors. Over the past 30 days, Mantis launched 3,000 DDoS attacks against almost a thousand Cloudflare customers, the company notes.

Most of the targets are organizations in the United States (20%) and the Russian Federation (15%), while victims in Turkey, France, Poland, Ukraine, the UK, Germany, Netherlands, and Canada account for percentages between 2.5% and 5%.

To help admins prepare for DDoS attacks, Cloudflare has issued a set of best preventative measures and guidance on how to respond to the attacks.

20.NIST goes with algorithm co-developed by Thales for post-quantum digital signatures

by Chris Burt
https://www.biometricupdate.com/202207/nist-goes-with-algorithm-co-developed-by-thales-for-post-quantum-digital-signatures

An algorithm co-developed by Thales has been selected as a post-quantum cryptography standard for digital signatures specifically for its ability to withstand future attacks from quantum computers.

The U.S. National Institute of Standards and Technology chose the Falcon algorithm for its extremely high security and bandwidth efficiency, Thales says. The selection concludes a five-year global competition to find ways of protecting digital signatures. The challenge drew 82 participants from 25 countries.

Digital signatures are widely used to confirm the authenticity of digital messages or digital identity documents.

The algorithm will be included in the post-quantum cryptography standards that NIST is expected to define in the next two years.

Falcon was developed in collaboration with the University of Rennes and PQShield from France, IBM researchers in Switzerland, Canada's NCC Group, and Qualcomm and Brown University in the U.S. Thales claims to be the only technology company taking part in the competition to serve the defense, aerospace and digital identity markets.

NIST chose another two algorithms as standards for digital signatures and a fourth for public key encryption and a key encapsulation mechanism.

Thales has been working on post-quantum cryptography research since 2013, Pierre-Yves Jolivet, the multinational's vice president of cyber defense products.

"Selection of the Falcon algorithm by NIST is great recognition of the excellent co-development work and expertise of our crypto teams," according to Jolivet.

"We will pursue our on-going research in France and Europe to develop innovative, trusted solutions that will be quantic-resistant, without compromising performance." Jolivet said the company is helping customers transition to the next generation of security, hopefully, to avert a "crypto-apocalypse."

A report published by Eurosmart in late 2021 argued that quantum computing could threaten the security of digital ID documents, including those with embedded biometric data.

21.Quantum Computing's Time is Coming

by Doug Finke
https://quantumcomputingreport.com/quantum-computings-time-is-coming/

So, is quantum computing ready to take off and disrupt industries as we know them? As an analyst and publisher about all things quantum, I hear variations of this question every day. My response is to fall back on the decades-old "Amara's Law," which states that: "We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."

In other words, I'm excited about the prospects, but cautious about overpromising revolutionary breakthroughs anytime soon.

First, what exactly is quantum computing? It's an emerging technology that uses quantum mechanics to run calculations. Quantum computers leverage the quantum mechanical phenomena of superposition, entanglement, and interference that allow the creation of new types of algorithms that can perform certain calculations much faster than classical computers.

Governments are taking notice. China has announced plans to invest $15.3 billion in quantum computing over the next five years with the E.U. and U.S. are putting up more than $7.2 billion and $1.9 bil-

lion, respectively. Other countries, including Japan, the U.K., India, and Canada are also funding quantum technology with over a billion dollars each. Investors are, too. Investments in quantum start-tups crossed $1.4 billion in 2021, more than double the year before figure, according to McKinsey.

Entering the 'Quantum Ready' Phase

Although the current generation of quantum computers are not yet powerful enough to surpass the capabilities of classical computer for commercially relevant applications, quantum technology is advancing very rapidly, and we do expect that a few quantum applications to become viable in the next 2-3 years. Many companies are seeking a competitive advantage in their industry by initiating quantum programs now in order to get familiar with the technology and take advantage of it when the more powerful processors are available. A study last year of over 500 corporate managers by Classiq, a quantum software company, found that 89.8% believe IT departments should have a budget specifically for quantum computing technologies, and 61.9% report that their company has already allocated a budget for quantum computing.

A critical challenge with quantum computing technology lies in the relatively high error rates associated with the quantum qubit gates due to their extreme sensitivity to disturbances from the outside environment. Researchers are working intensely to combat this and the industry views that quantum computing development will fall into two phases.

The current phase is called NISQ, standing for Noisy, Intermediate Scale Quantum. Although engineers cannot completely eliminate the noise that causes inaccuracies in the system, they are developing techniques to reduce it. And clever programmers are developing algorithms that can produce useful solutions to certain application problems despite the remaining level of noise. We expect that there will be a few commercial applications that will become viable soon with NISQ-level computers.

The next phase is called Fault Tolerant Quantum Computing where engineers develop error correction algorithms that will effectively eliminate the problem of errors for the programmer so they can develop many more commercial quantum applications. Creating these fault tolerant quantum computers is still a difficult challenge and will require much larger processors than exist today. However, we do expect that several organizations will succeed and make these machine available by the end of the decade.

Where Quantum Computing Can Make a Difference

Although quantum computers won't do much for common consumer applications like email, web browsing or accounting, there are still many exciting applications where it should make a difference.

Quantum computing will only be commercially useful when it can solve certain types of problems that are impossible or extremely difficult for a classical computer to solve, a situation we call "Quantum Advantage." Using a quantum computer to simulate quantum-level chemical reactions is a very natural and extremely important class of applications. Applications of this type include drug discovery, material design, and key problems associated with climate change like carbon capture and solar energy conversion.

Optimization will be another major type of applications where quantum technology can provide benefit. Many industries will find they can better optimize their company's operations through quantum computing. For example, the financial industry will be able to develop improved portfolio optimizations, credit risk analysis, Monte Carlo modeling, and trading strategies. Any organization that deals with logistics will be able to use quantum technology for things like vehicle routing, network optimization, or optimizing process and manufacturing flows.

And a third type of application will be in quantum machine learning capabilities. Quantum can potentially provide significant speed-ups or improvement in accuracy versus a classical computing approach for various machine learning problems. These can include such things as fraud detection and money laundering protection for financial companies, image recognition, and training neural networks.

Quantum and Classical Computers Will Be Used in Tandem

Will quantum computers ever replace classical computers? Not likely. Although quantum computers may eventually displace some high-performance classical computers, there are a great many tasks that a quantum computer is not well suited for, such as reading email, running a website, maintaining a financial transaction database, browsing the internet, calculating bank balances, and most of the other tasks we perform on computers today.

In fact, many people believe that most quantum computing will be accomplished with quantum and classical working together. They believe it will be similar to how GPU's are used today as coprocessors that support the main classical processor.

Quantum's Encryption Issue

One issue people are talking about today is a threat quantum computing could pose in the distant future. As quantum computers gain more power, experts believe they'll be able to break the RSA encryption computers use on the internet today. This won't happen right away, but it could occur 10-15 years from now. This poses a problem for data that has a long shelf life – like medical records. There are solutions called Post Quantum Cryptography (PQC) and QKD (Quantum Key Distribution). Corporate leaders should start planning for this because they may have to upgrade thousands of systems in their organization to make them quantum resistant.

Developing a Quantum Work Force

While work still needs to be done on quantum's hardware, software, algorithm and system designs, skills development also needs to be put high on the priority list. The lack of availability of trained people could be the thing that limits the growth of the industry. Luckily, governments and private industry groups are starting to introduce solutions to the problem and get people trained.

A number of organizations, including the National Science Foundation, the National Institute of Standards and Technology (NIST), the White House Quantum Coordination office and the Quantum Economic Development Consortium (QED-C) all have programs for helping to build up a quantum work

force. I work on a QED-C initiative designed to inspire students to get involved and help professors put together curricula. It will take a lot of work, but progress is being made.

Recommendations

While quantum's true impact is still likely a few years away, there are things IT managers can do to prepare for a quantum future.

- Prepare for the RSA break: Even though it's purely a defensive move, IT managers should start a program right now. Just converting systems to become quantum resistant from using RSA-based encryption to using a new approach will take many years. It will take a large enterprise 5-10 years to find all systems and convert them to make them quantum resistant.

- Take inventory of IT systems: Find out what data you need to protect that will have a long shelf life and find out what systems work with that type of data.

- Identify quantum use cases: Survey all the various IT processes within the organization and see which ones might be amenable to being accelerated or improved by using quantum technology.

- Upgrade quantum skills: As quantum computers develop, IT managers will need skilled operators. Start scoping out job roles for a quantum environment and look for candidates to fill those rolls. Also, evaluate whether it makes sense to bring in outside consultants who can help you on your journey to implement quantum technologies within your organization.

Conclusion

To the quantum enthusiasts who hope the computers will change the world right away, here's my advice: Be patient. Quantum is coming. We're seeing incremental breakthroughs every year, and dollars are being invested to advance the technology. Also, don't underestimate its future impact. Start making moves today to take advantage of a technology that will be very helpful tomorrow.

22.How quantum-safe cryptography will ensure a secure computing future

by World Economic Forum

https://europeansting.com/2022/07/08/how-quantum-safe-cryptography-will-ensure-a-secure-computing-future/

The National Institute of Standards and Technology (NIST), a US government lab that publishes standards for government agencies to safely use cryptography, has just announced the winners of a six-year-long competition to create quantum-safe algorithms.

Why is that important? Medical, financial, and health records — for sensitive data protection, encryption and authentication is crucial. Today it's pretty robust, but future quantum computers could change that. It's been said time and time again that this emerging, powerful technology based on nature's quantum intricacies could break cryptography, wreaking havoc in our digital lives. Still, this is unlikely to happen.

How can cryptography turn quantum-safe?

To prevent this from happening, researchers have been working on a technology called **quantum-safe cryptography**. These cutting-edge constructions are based on different mathematical approaches to those widely adopted today. For example, techniques rooted in lattice and isogeny-based mathematics.

With the winning quantum-resistant cryptographic systems NIST has just announced, the world could soon be safe from any potential threat of quantum computers of the future.

Scientists working at IBM took part in a lot of winning algorithms. One of the winning schemes that has been developed by IBM researchers and their partners is the CRYSTALS-Kyber public-key encryption scheme. The other ones are the CRYSTALS-Dilithium, Falcon, and SPHINCS+ digital signature schemes, which were also developed by IBM scientists and collaborators.

Also, a fifth scheme created by IBM, the so-called SIKE encryption scheme, has been earmarked for further study and possible later standardisation. When adopted, the new schemes should be able to keep computing systems safe from quantum hacking. Organisations around the world should consider migrating to them as soon as possible.

NIST is a US government lab that publishes standards for government agencies to safely use cryptography. Relied on by most public and private organizations globally, these standards detail how to use different cryptographic algorithms so that a user's computer securely communicates with the computer of the intended recipient. They are the basis for today's secure global communications – be it making a purchase on the web or transferring sensitive data.

Quantum-safe algorithms for new security standards

But that only applies to classical computers. Quantum computers are different.

Quantum computers harness the properties of quantum mechanics and promise to solve, in the future, specific problems beyond the power of classical machines. And while a quantum computer could help us create new materials much more efficiently than we do today while getting a better handle on financial market fluctuations and so much more, they could also break some of NIST's current standardized crypto algorithms, exposing the sensitive data they were used to encrypt.

This is why we need to adopt new standards to get ahead of this issue.

For example, at IBM, the research into this new type of quantum-safe encryption started around

2015. One of the top cryptographers at their lab in Zurich, Vadim Lyubashevsky, had just moved to Switzerland from France and, having obtained funding from the Swiss National Foundation, kicked off the research. He wasn't going at it alone: the funding allowed him to hire several key people, including a then-PhD student at ETH, Gregor Seiler, who later became instrumental in building lattice-based cryptosystems.

And then in 2016, NIST sent crypto ripples across industry and academia, having launched an international competition to develop new quantum-resistant algorithms. Several companies around the world have joined the arena, while a number of top people across the crytpography spectrum, from theoreticians to practitioners, worked either at IBM or with IBM to contribute to the recently announced new schemes by NIST.

Quantum-safe crypto 101

Today, there are two types of cryptography: **symmetric and asymmetric**.

It's the asymmetric one, commonly used for our day-to-day communication by secure web browsers, chats, VPNs and so on, that could be cracked by a quantum computer. It relies on a private and a public key that is mathematically linked, with the public key responsible for encryption or verification. The private key is only intended for a specific party decrypting or signing the data.

Many asymmetric crypto algorithms rely on a maths problem called prime factorisation, and the longer the key – the more bits it contains – the more difficult it is to break the encryption. And while today's computers can't break these algorithms, a quantum computer could – thanks to Shor's algorithm, developed by Peter Shor in 1994. That's because factoring numbers, no matter how long a sequence is, is child's play for a quantum computer with millions of qubits.

Today, crypto protocols such as SSL, Transport Layer Security and HTTPS are based on so-called cryptographic "primitives" – low-level cryptographic algorithms. These include digital signatures, authentication schemes and encryption schemes. But these protocols become useless if the crypto primitives are compromised.

That's where lattice cryptography can help. It relies on the area of maths dubbed "geometry of numbers," where data is hidden inside lattices, complex algebraic structures. While it's easy to create a point in space that is close to the lattice, the hardness of lattice-based cryptography is because it's difficult to go in the opposite direction. Finding the nearest place in the lattice from a point in space requires time that is exponential in the dimension of the lattice.

This problem has been studied since the 1970s and an efficient algorithm for it would have many applications in a lot of important areas. It has also received a lot of attention from the quantum algorithms community.

Securing the future

NIST has announced that it will standardize the winning cryptosystems by 2024. It means that the

US government will start adopting these schemes and requiring that their suppliers use them too.

There probably won't be just one standard. As we've seen with classical cryptography, there are many different standards being used for scientific or political reasons. Eventually with time, if one standard is clearly better, people typically gravitate towards it for new systems.

Today, we are still at a very early stage of quantum-safe crypto. The needs of people who consume crypto might be different in a decade. They might value some characteristics more than the ones being emphasized today and might want to use schemes optimal for those specific purposes. Having said this, it's hard to imagine something being faster than lattice cryptography which is being envisioned by many experts to be used across different fields in the future.

It is crucial for organisations worldwide to understand the risks of quantum computers and to realise that solutions thanks to NIST's selection of quantum-safe standards are becoming available. They should start preparing today.

23.ID Quantique and CryptoNext partner to deliver next-gen, quantum-safe messaging

by Catherine Simondi & Christian D'orival

https://www.idquantique.com/idq-and-cryptonext-partner-to-deliver-quantum-safe-messaging/?utm_term=ID%20Quantique%20and%20CryptoNext%20partner%20to%20deliver%20next-gen%2C%20quantum-safe%20messaging&utm_campaign=Quantum%20Era%20Security%20Times%20July%202022&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%20July%202022-_-ID%20Quantique%20and%20CryptoNext%20partner%20to%20deliver%20next-gen%2C%20quantum-safe%20messaging

Geneva based ID Quantique SA (IDQ), a global leader in Quantum Cybersecurity Solutions, and Paris based CryptoNext Security SAS (CryptoNext), a pioneer and leader in Post-Quantum Cryptography (PQC), today announce their partnership to offer an effective and long-term Quantum-Safe Communication Solution for mobile phone users.

Mobile communications have become fully integrated in today's hyper-connected world, where huge volumes of data, much of it sensitive in nature, flow everywhere. At the same time, significant investment into quantum computing technology has seen significant advances being made, bringing the dawn of the quantum computing age ever closer.

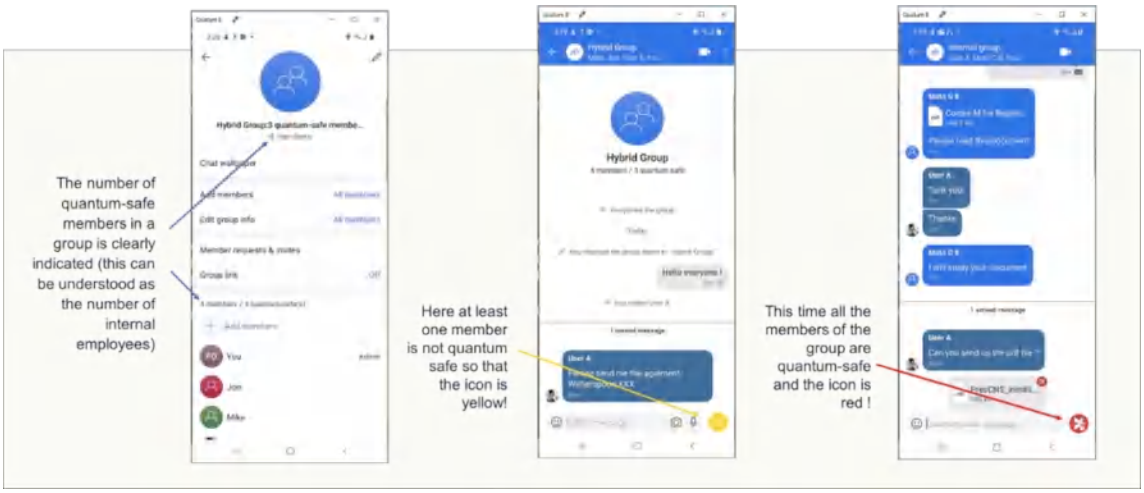
The arrival of quantum computers is anticipated with enthusiasm and apprehension in equal measure.

Apprehension because a quantum computer will be capable of breaking today's cryptographic infrastructure with ease. This has created the need for a new approach to cybersecurity, and new solutions in this forthcoming era. But this isn't just a problem for tomorrow, it represents a very real threat today. Organisations must also protect long-life, high-value data against potential "harvest now, decrypt later" attacks. The need to act now is widely acknowledged by national security agencies, including the NSA and the National Institute of Standards and Technologies (NIST) in the US, ANSSI in France and the BSI in Germany.

In a clear move to address the challenges of long term, quantum-resistant data protection, solutions are being developed that leverage existing quantum technologies, such as Quantum Random Number Generation (QRNG) and Post-Quantum Cryptography (PQC).

Following a successful test project at NATO, IDQ and CryptoNext have joined forces to bring to market the next generation of quantum-secured communications solutions. Leveraging a combination of their world-leading QRNG and PQC technologies, the aim is to provide essential support to end-users plus systems integrators and specialized solutions vendors.

The solution is a quantum-safe messaging application for mobile communications. It combines Cryptonext's Quantum-Safe Messaging Application Plugin (C-QS-MS) and Quantum Safe Library (C-QSL) with automated detection of ID Quantique's QRNG Microchip. Embedded in some brands of smartphones, the QRNG Microchip provides the most reliable source of entropy for any cryptographic process. The result is an end-to-end text, file exchange, voice and video call Quantum-Safe messaging solution. The application is transparent to the user and comes with detailed group management features to efficiently manage the security of specific groups.



The solution aims at enabling governments, enterprises and organizations of all types to manage sensitive communications for specific groups of people, such as executive teams, and/or specific projects.

"We are delighted to team with CryptoNext Security, a recognized leader in Post-Quantum Cryptography to leverage our market leading QRNG chip integrated into smart phones and offer our customers the most secure messaging application."

Gregoire Ribordy, CEO and co-founder, ID Quantique

"It is great honor for us to be recognized by and team up with IDQ, a clear market leader in QRNG technologies with proven track record in deployment and supporting customers with quantum-safe crypto solutions."

Florent Grosmaitre, CEO CryptoNext Security

24.The cryptopocalypse is nigh! NIST rolls out new encryption standards to prepare

by Dan Goodin

https://arstechnica.com/information-technology/2022/07/nist-selects-quantum-proof-algorithms-to-head-off-the-coming-cryptopocalypse/

Decision will be binding on many companies and change the way they protect your data.

In the not-too-distant future—as little as a decade, perhaps, nobody knows exactly how long—the cryptography protecting your bank transactions, chat messages, and medical records from prying eyes is going to break spectacularly with the advent of quantum computing. On Tuesday, a US government agency named four replacement encryption schemes to head off this cryptopocalypse.

Some of the most widely used public-key encryption systems—including those using the RSA, Diffie-Hellman, and elliptic curve Diffie-Hellman algorithms—rely on mathematics to protect sensitive data. These mathematical problems include (1) factoring a key's large composite number (usually denoted as N) to derive its two factors (usually denoted as P and Q) and (2) computing the discrete logarithm that key is based on.

The security of these cryptosystems depends entirely on how difficult it is for classical computers to solve these problems. While it's easy to generate keys that can encrypt and decrypt data at will, it's impossible from a practical standpoint for an adversary to calculate the numbers that make them work.

In 2019, a team of researchers factored a 795-bit RSA key, making it the biggest key size ever to be solved. The same team also computed a discrete logarithm of a different key of the same size.

The researchers estimated that the sum of the computation time for both of the new records was about 4,000 core-years using Intel Xeon Gold 6130 CPUs (running at 2.1 GHz). Like previous records, these were accomplished using a complex algorithm called the Number Field Sieve, which can be used to perform both integer factoring and finite field discrete logarithms.

Quantum computing is still in the experimental phase, but the results have already made it clear it can solve the same mathematical problems instantaneously. Increasing the size of the keys won't help, either, since Shor's algorithm, a quantum-computing technique developed in 1994 by American mathematician Peter Shor, works orders of magnitude faster in solving integer factorization and discrete

logarithmic problems.

Researchers have known for decades these algorithms are vulnerable and have been cautioning the world to prepare for the day when all data that has been encrypted using them can be unscrambled. Chief among the proponents is the US Department of Commerce's National Institute of Standards and Technology (NIST), which is leading a drive for post-quantum cryptography (PQC).

On Tuesday (05 Jul 2022), NIST said it selected four candidate PQC algorithms to replace those that are expected to be felled by quantum computing. They are: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+.

CRYSTALS-Kyber and CRYSTALS-Dilithium are likely to be the two most widely used replacements. CRYSTALS-Kyber is used for establishing digital keys that two computers that have never interacted with each other can use to encrypt data. The remaining three, meanwhile, are used for digitally signing encrypted data to establish who sent it.

``CRYSTALS-Kyber (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications," NIST officials wrote. "FALCON will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. SPHINCS+ will also be standardized to avoid relying only on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures."

The selections announced today are likely to have significant influence going forward.

``The NIST choices certainly matter because many large companies have to comply with the NIST standards even if their own chief cryptographers don't agree with their choices," said Graham Steel, CEO of Cryptosense, a company that makes cryptography management software. "But having said that, I personally believe their choices are based on sound reasoning, given what we know right now about the security of these different mathematical problems, and the trade-off with performance."

Nadia Heninger, an associate professor of computer science and engineering at the University of California, San Diego, agreed.

``The algorithms NIST chooses will be the de facto international standard, barring any unexpected last-minute developments," she wrote in an email. "A lot of companies have been waiting with bated breath for these choices to be announced so they can implement them ASAP."

While no one knows exactly when quantum computers will be available, there is considerable urgency in moving to PQC as soon as possible. Many researchers say it's likely that criminals and nation-state spies are recording massive amounts of encrypted communications and stockpiling them for the day they can be decrypted.

25.NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

by Chad Boutin

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools that are designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day — such as online banking and email software. The four selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years.

"Today's announcement is an important milestone in securing our sensitive data against the possibility of future cyberattacks from quantum computers," said Secretary of Commerce Gina M. Raimondo. "Thanks to NIST's expertise and commitment to cutting-edge technology, we are able to take the necessary steps to secure electronic information so U.S. businesses can continue innovating while maintaining the trust and confidence of their customers."

The announcement follows a six-year effort managed by NIST, which in 2016 called upon the world's cryptographers to devise and then vet encryption methods that could resist an attack from a future quantum computer that is more powerful than the comparatively limited machines available today. The selection constitutes the beginning of the finale of the agency's post-quantum cryptography standardization project.

"NIST constantly looks to the future to anticipate the needs of U.S. industry and society as a whole, and when they are built, quantum computers powerful enough to break present-day encryption will pose a serious threat to our information systems," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "Our post-quantum cryptography program has leveraged the top minds in cryptography — worldwide — to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information."

Four additional algorithms are under consideration for inclusion in the standard, and NIST plans to announce the finalists from that round at a future date. NIST is announcing its choices in two stages because of the need for a robust variety of defense tools. As cryptographers have recognized from the beginning of NIST's effort, there are different systems and tasks that use encryption, and a useful standard would offer solutions designed for different situations, use varied approaches for encryption, and offer more than one algorithm for each use case in the event one proves vulnerable.

"Our post-quantum cryptography program has leveraged the top minds in cryptography — worldwide — to produce this first group of quantum-resistant algorithms that will lead to a standard and signifi-

cantly increase the security of our digital information." — NIST Director Laurie E. Locascio

Encryption uses math to protect sensitive electronic information, including the secure websites we surf and the emails we send. Widely used public-key encryption systems, which rely on math problems that even the fastest conventional computers find intractable, ensure these websites and messages are inaccessible to unwelcome third parties.

However, a sufficiently capable quantum computer, which would be based on different technology than the conventional computers we have today, could solve these math problems quickly, defeating encryption systems. To counter this threat, the four quantum-resistant algorithms rely on math problems that both conventional and quantum computers should have difficulty solving, thereby defending privacy both now and down the road.

The algorithms are designed for two main tasks for which encryption is typically used: general encryption, used to protect information exchanged across a public network; and digital signatures, used for identity authentication. All four of the algorithms were created by experts collaborating from multiple countries and institutions.

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms CRYSTALS-Dilithium, FALCON and SPHINCS+ (read as "Sphincs plus"). Reviewers noted the high efficiency of the first two, and NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. The third, SPHINCS+, is somewhat larger and slower than the other two, but it is valuable as a backup for one chief reason: It is based on a different math approach than all three of NIST's other selections.

Three of the selected algorithms are based on a family of math problems called structured lattices, while SPHINCS+ uses hash functions. The additional four algorithms still under consideration are designed for general encryption and do not use structured lattices or hash functions in their approaches.

While the standard is in development, NIST encourages security experts to explore the new algorithms and consider how their applications will use them, but not to bake them into their systems yet, as the algorithms could change slightly before the standard is finalized.

To prepare, users can inventory their systems for applications that use public-key cryptography, which will need to be replaced before cryptographically relevant quantum computers appear. They can also alert their IT departments and vendors about the upcoming change. To get involved in developing guidance for migrating to post-quantum cryptography, see NIST's National Cybersecurity Center of Excellence project page.

All of the algorithms are available on the NIST website.

26.End-to-End Encryption's Central Role in Modern Self-Defense

by Lily Hay Newman
https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/end-to-end-encryption-abortion-privacy/amp

With abortion set to be criminalized in more than half the US, encryption has never been more important for protection—and civil disobedience.

A number of course-altering US Supreme Court decisions last month—including the reversal of a constitutional right to abortion and the overturning of a century-old limit on certain firearms permits—have activists and average Americans around the country anticipating the fallout for rights and privacy as abortion "trigger laws," expanded access to concealed carry permits, and other regulations are expected to take effect in some states. And as people seeking abortions scramble to protect their digital privacy and researchers plumb the relationship between abortion speech and tech regulations, encryption proponents have a clear message: Access to end-to-end encrypted services in the US is more important than ever.

Studies, including those commissioned by tech giants like Meta, have repeatedly and definitively shown that access to encrypted communications is a human rights issue in the digital age. End-to-end encryption makes your messages, phone calls, and video chats unintelligible everywhere except on the devices involved in the conversations, so snoops and interlopers can't access what you're saying—and neither can the company that offers the platform. As the legal climate in the US evolves, people who once thought they had nothing to hide may realize that era is now over.

"There are plenty of people in the US for whom it has always been true that the state wasn't really helping them and was mostly harming them," says Riana Pfefferkorn, a research scholar at the Stanford Internet Observatory. "But for those who are now losing faith in traditional institutions of government, it provides room for them to say, 'OK, what technologies exist for taking back some control?'"

Over the past decades, law enforcement officials around the world have increasingly marked encryption as a hindrance to investigations and, therefore, a threat. The US Department of Justice and other agencies worldwide have campaigned to undermine encryption features with backdoors or make it economically infeasible for companies to offer the protection. While it is important to prevent violence and prosecute activity like the distribution of child sexual abuse materials, researchers consistently note that criminals will deploy and use encryption to protect their data whether the tools are legal or not—as has been the case with terrorist groups like Al Qaeda and ISIS.

Moxie Marlinkspike, the cryptographer who founded the open source, end-to-end encrypted messaging service Signal, explored the question of criminality and access to secure communications in a blog post nearly 10 years ago. "Police already abuse the immense power they have, but if

everyone's every action were being monitored, and everyone technically violates some obscure law at some time, then punishment becomes purely selective," he wrote. "Those in power will essentially have what they need to punish anyone they'd like, whenever they choose."

The potential for laws to change abruptly and completely was on display last month in the Supreme Court's New York State Rifle & Pistol Association v. Bruen decision that struck down a century-old concealed carry licensure law with implications for similar laws in other states. And Dobbs v. Jackson Women's Health Organization instantly banned abortion in many states—a move that means people around the country who were previously law-abiding may now be seeking life-or-death treatment in violation of the law. Furthermore, in restrictive states, people who aid someone who receives an abortion or who are simply close to a patient could now be subject to law enforcement surveillance and investigation, regardless of whether they are ultimately charged and prosecuted.

Meanwhile, anti-encryption initiatives in the US, including proposed legislation like the Earn It Act, continue to pit law enforcement against technical protections. Pfefferkorn is clear about the divide. "You really can't be pro-choice and anti-encryption at this point," she says.

Researchers point out that encryption is often thought of in the context of enabling free speech, but it can also be looked at through the lens of self-defense.

"Effective, uncensorable, secret communications are certainly far more valuable to resistance movements than small arms are," says computer security consultant Ryan Lackey. "If you had magic, secure telepathy between everyone in your organization, in a civil war or resistance scenario where some of your allies were inside the opposition, you wouldn't need a single gun to win."

Lackey points out that there are parallels between encryption and firearms, as laid out in the Second Amendment, an observation that others have explored at times. The crucial element, though, is the connection to a right to self-defense, which the Supreme Court's Second Amendment absolutists cite repeatedly as the law's "central component."

Beyond end-to-end encryption's ability to protect people from their government, police, and prosecutors, it also protects them from other people who seek to enact harm, be they criminal hackers or violent extremists. While equating encryption to a weapon misconstrues its function—it's much more shield than sword—these defenses remain the most powerful tool people everywhere have to protect their digital privacy. And a clear parallel can be drawn to the fervor with which gun advocates embrace their right to bear arms.

Stanford's Pfefferkorn points out that it is logical and necessary for abortion providers, patients, or anyone who is pro-choice to embrace and defend encryption in general, but particularly so in light of the overturning of Roe v. Wade. She adds that in this moment, when the Supreme Court is reversing decades of established precedent on a variety of issues at once, the most important generalizable takeaway is the benefits of access to end-to-end encryption, and the necessity of preserving that access.

"Laws can change. Social rules can change. The perfectly harmless conversation you had yesterday might come back to hurt you years from now," says Johns Hopkins cryptographer Matthew Green.

"That's why we don't write down every spoken conversation and keep it forever. Encryption is just a way to give digital communications the same basic protections."

Twenty-six states have either criminalized abortion, will do so, or are likely to take that step. How those laws will be enforced remains unknown. What's certain is that millions of people who had nothing to hide before the Supreme Court's June 24 decision now face the prospect of potential targeting, surveillance, and even prison over their reproductive health. And comprehensive encryption will be essential to their self-defense. As Signal's Marlinspike said during a panel discussion at the 2016 RSA security conference in San Francisco, "I actually think that law enforcement should be difficult … I think it should actually be possible to break the law."

27.Where Next for Quantum Computing and Cybersecurity?

by Dan Lohrmann

https://www.govtech.com/blogs/lohrmann-on-cybersecurity/where-next-for-quantum-computing-and-cybersecurity

A CNBC headline last month grabbed my attention: The race toward a new computing technology is heating up — and Asia is jumping on the trend.

I immediately wanted to know: What technology?

The answer came in the first summary bullet: "Japan has made key advancements in the quantum computer race, India has developed its own strategy for the technology and debates are simmering over whether China has surpassed the U.S. on some fronts."

WHY QUANTUM COMPUTING?

I have been intrigued by advances in quantum computing for several years. I wrote this blog on the topic back in early 2020, before the pandemic took hold.

Here's an excerpt: "This past week, the Washington Post wrote that the U.S. hatches plan to build a quantum Internet that might be unhackable. The new network would sit alongside the existing web, offering a more secure way to send and process information."

So why am I so intrigued by this topic? As I quoted from the Department of Energy (DOE) in 2020, "A quantum Internet would 'rely on the laws of quantum mechanics to control and transmit information more securely than ever before,' according to DOE. The department's 17 national labs will work on the secure network, which could be used for science, industry and national security."

Meanwhile, two weeks ago, Brookings.edu published this piece on "How U.S. policymakers can enable

breakthroughs in quantum science": "the field of quantum information science and technology (QIST), stands at the cusp of a series of breakthroughs that could finally bring quantum technology — and the great benefits it will likely bring with it — into the mainstream. But progress in QIST is fragile, and sustaining this progress requires investment and coordination by the U.S. government and a continued policy of openness toward the scientists that will deliver these breakthroughs. …

"Just as federal investment in the 1960s to the 1980s incubated the breakthrough technologies that made today's Internet possible, U.S. policymakers now have an opportunity to facilitate major advances in quantum computing — and make them as widely available as possible. As with the Internet, the development of a quantum Internet and associated systems like quantum computers and quantum sensors should be aimed initially at providing new capabilities to scientists and other researchers to make new discoveries. To this end, it is important to provide open access to those who wish to use federally supported infrastructure for research. Private companies have a significant role to play by making available open platforms for quantum computing, like IBM's Quantum Experience."

One more recent piece to point out comes from FedTech Magazine: "Much of the budget growth is for activities related to the National Quantum Initiative Act, signed into law in 2018. This includes the establishment of quantum consortia by the National Institute of Standards and Technology; Quantum Leap Challenge Institutes by the National Science Foundation; National Quantum Information Science Research Centers by the Department of Energy; and the coordination and strengthening of core QIS programs across multiple agencies, according to the report."

QUANTUM COMPUTING AND CYBERSECURITY

There are many reports that describe the potential impacts of quantum computing on the cyber industry. This article describes how to prepare now for a post-quantum world.

Here's an excerpt: "So how does a business become post-quantum-prepared? Firstly, do not wait until NIST issues its standard. The time to become post-quantum-prepared is now. Begin by determining what data is most likely to be sought out by cyber criminals. …

"Keeping the amount of important/vulnerable data in mind, a strategy should be developed to address the business's priorities for using quantum resistant encryption. Next, develop your priorities for quantum-resistant encryption while making a plan to upgrade your infrastructure for the next several years."

FINAL THOUGHTS

There are certain technology topics that we need to keep checking in on to see advances and next steps, like autonomous vehicles, the metaverse and artificial intelligence.

And quantum computing needs to stay near the top of that list throughout the 2020s.

28.World's first quantum computer integrated circuit

https://www.futuretimeline.net/blog/2022/07/3-worlds-first-quantum-computer-integrated-circuit.htm

The world's first quantum computer integrated circuit has been demonstrated at the University of New South Wales (UNSW), Australia.

Silicon Quantum Computing (SQC) is an Australian company formed in May 2017 by a collaboration including UNSW Sydney, the Commonwealth of Australia, Telstra Corporation, and the State of New South Wales. Funded with A$83 million (US$57m), it acquired a portfolio of world-leading quantum computing intellectual property (IP) and has been at the forefront of global efforts to bring commercial-scale quantum computers to market.

SQC comprises a world-class team of quantum scientists, engineers, and technicians, as well as specialist equipment and laboratories at UNSW. In addition to its core processor technology, the company is developing a "full stack" quantum computer to ensure it can deliver a useful and manufacturable device.

In 2012, a team at UNSW created the first ever quantum transistor, just a single atom in size. Following the establishment of SQC and further years of research and development, they have just announced their biggest milestone to date: the world's first integrated circuit manufactured at the atomic scale. Furthermore, this has been achieved two years ahead of schedule.

The researchers used a scanning tunnelling microscope in an ultra-high vacuum to place quantum dots on the chip. This required extraordinary precision – at the sub-nanometre scale. For the device to work, the exact number of phosphorus atoms had to be determined for each dot, as well as the exact spacing between each one. This is needed so that their energy levels are perfectly aligned, electrons pass easily through them, and quantum coherence is maintained. The chip features a total of 10 quantum dots, as seen below.

They then used this analogue quantum processor to accurately model the quantum states of a small, organic polyacetylene molecule – definitively proving the validity of the company's technology for modelling quantum systems.

"This is a major breakthrough," said Michelle Simmons, Professor of Quantum Physics at UNSW, and the founder of SQC, who described the quantum circuit as the biggest result of her career. "Today's classical computers struggle to simulate even relatively small molecules due to the large number of possible interactions between atoms. The development of SQC's atomic-scale circuit technology will allow the company and its customers to construct quantum models for a range of new materials, whether they be pharmaceuticals, materials for batteries, or catalysts. It won't be long before we can start to realise new materials that have never existed before."

"With critical and emerging technologies such as quantum hardware, stakeholders gain huge confidence from the technical team's ability to meet stated milestones. To reach such a landmark two years ahead of schedule is a triumph," said Stephen Menzies, SQC Chairman. "SQC's engineers are now scaling the technology to address more industrially relevant molecules and as a business we look forward to developing targeted industry partnerships to address their simulation needs."

The ability to observe precisely how molecules function at the atomic scale would remove a lot of the guesswork in the creation of new materials. To simulate a penicillin molecule with 41 atoms, a classical computer would need 10^{86} transistors, which is more transistors than there are atoms in the observable universe. But a quantum computer would require a processor with only 286 qubits (quantum bits).

The next technical milestone for SQC is expected to be a 100-qubit quantum device. In addition to its quantum circuit breakthrough, the company recently announced the launch of A$130 million in Series A funding for development, operations, and strategic activities from 2023 to 2028.

"SQC's unique approach ensures the scalability and quality of our tech. Combined with our ability to manufacture in-house and secure talent and partnerships, we're on track to deliver useful commercial quantum computing by 2028," said Menzies.

