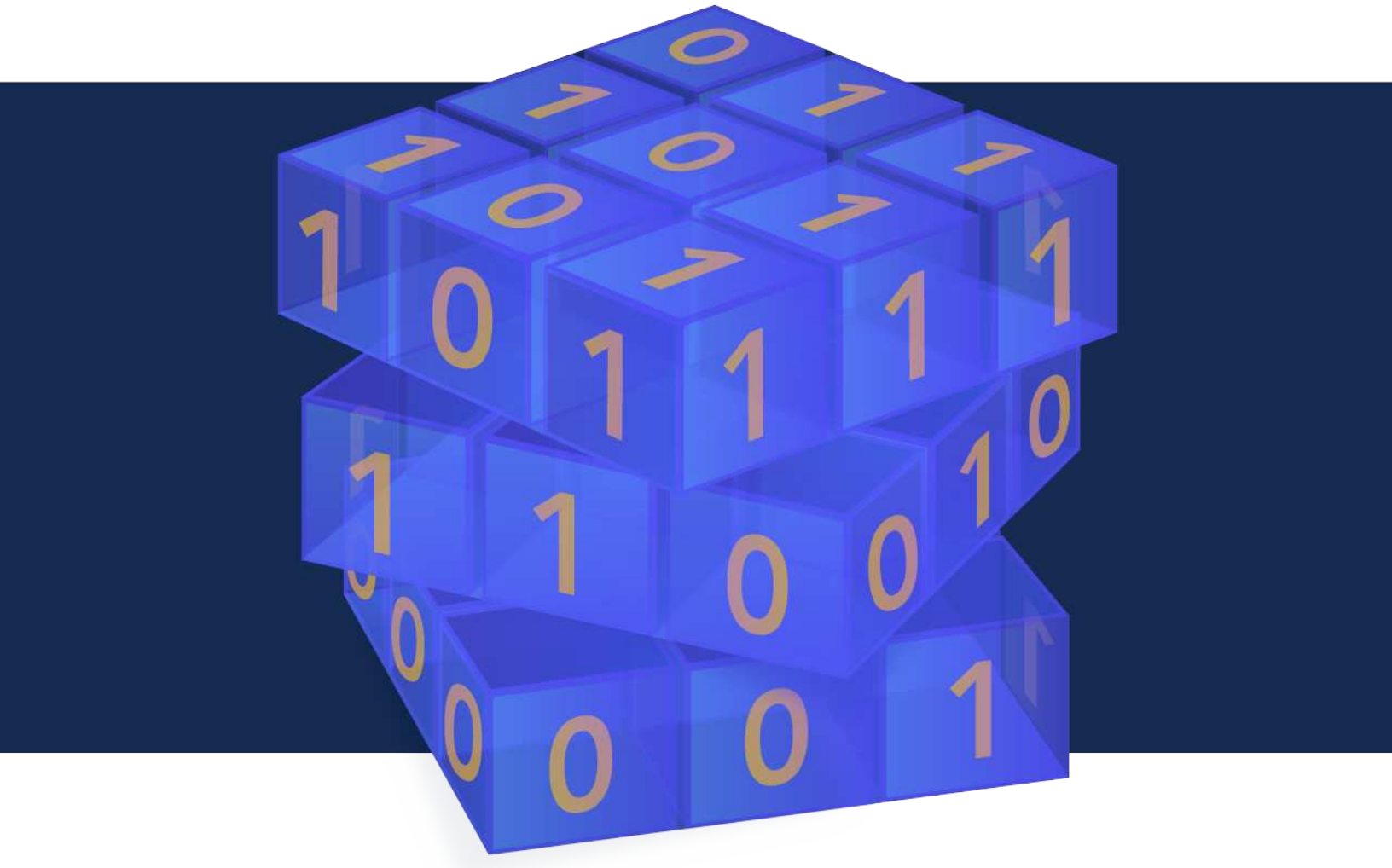
Crypto News

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

June 01, 2022



1.Editorial

It's that time again! Here's your latest issue of Crypto News! There are several interesting articles in this issue. Take article #16 for example which puts forth an intriguing argument that "quantum computing just might save the planet". A number of corporations and countries pledged to reduce emissions by 2021 during the United Nations Climate Change Conference. When planning what they should do to meet the goals set, these organizations and countries may want to consider quantum computing as a part of their solution sets. It may just save us all! Another interesting article this month is #32. Winnti, a Chinese hacking group, is behind one of the most damaging cyber campaigns in the recent past. They have been stealing intellectual property from global organizations since 2019 until they were recently detected. What are their plans with this data? Was the data at least encrypted at rest when they stole it? If the answer to the second question is yes, then the financial losses are not immediate. But, with the rise of quantum computing, even encrypted data at rest that is stolen now won't be safe since post-quantum encryption wasn't utilized to protect it. Then the real danger and financial impact will come several years in the future when the hackers can use quantum computers to decrypt the stolen data. As a Security professional, I know that caught my attention. As always, happy reading!

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

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

2.First demonstration of universal operations on an error-free quantum computer

by Evrim Yazgin
https://cosmosmagazine.com/technology/error-free-quantum-computer/

Quantum computers are ravaged by errors, but new research has shown how fault-free quantum computer can be built.

For years we have been told that quantum computing is just around the corner, with many advances suggesting that computers based on quantum mechanics will eventually supersede current computing technologies and open an array of new possibilities. Now, new research has developed the first functioning error-free quantum-computing system.

Using the complex and irregular quantum principles of superposition and entanglement to build a functioning computer is not easy. Current quantum machines, though representing huge leaps forward in

our understanding and technical abilities, are rife with errors.

Modern, non-quantum computers avoid faults in the processing and storage of information through high-quality manufacturing. But critical applications still require error-correction procedures based on redundancy of data.

Because of the nature of quantum mechanics, quantum computers are more susceptible to errors and data loss. So, quantum machines will always require error correction. But quantum mechanics also forbids the copying of quantum information, so redundancy has to be achieved by scattering logical quantum information into an "entangled state" comprising several physical systems – for example, multiple atoms.

Explained in a paper published in Nature, researchers implemented computational operations on two quantum bits (qubits). The qubits are part of an ion trap quantum computer comprising 16 trapped atoms. Each qubit's information was distributed over seven other atoms.

The team then executed the first-ever error-free universal computational operation on qubits.

What do they mean by "universal"? Using different permutations and configurations of two particular quantum logical gates, any possible operation is possible. The two gates are the controlled-NOT (CNOT) gate and the T-gate. "For a real-world quantum computer, we need a universal set of gates with which we can program all algorithms," explains Lukas Postler, an experimental physicist from the University of Innsbruck, Austria.

CNOT is an operation where the second qubit is flipped if – and only if – the first qubit is in the state 1 (instead of 0). The T-gate, which is particularly difficult to implement on fault-tolerant qubits, changes the phase of the target qubit.

"T-gates are very fundamental operations," says Markus Müller, theoretical physicist from RWTH Aachen University and Forschungszentrum Jülich in Germany. "They are particularly interesting because quantum algorithms without T-gates can be simulated relatively easily on classical computers, negating any possible speed-up. This is no longer possible for algorithms with T-gates."

Errors caused by the underlying physics when operations are made on qubits are detected and corrected in the researchers' machine.

"The fault-tolerant implementation requires more operations than non-fault-tolerant operations," says team leader and University of Innsbruck experimental physicist Thomas Monz. "This will introduce more errors on the scale of single atoms, but nevertheless the experimental operations on the logical qubits are better than non-fault-tolerant logical operations. The effort and complexity increase, but the resulting quality is better."

The experimental results were checked and confirmed using numerical simulations on classical computers. Now, two qubits does not a functioning, useable quantum computer make – most modern computers are 32- or 64-bit – but the team has demonstrated that error-free quantum computing is possible. The goal now is to expand their set-up to larger and more complicated, and hence more useful,

machines.

3.How randomly moving electrons can improve cyber security

by Indian Institute of Science
https://techxplore.com/news/2022-05-randomly-electrons-cyber.html

In October 2017, tech giant Yahoo! disclosed a data breach that had leaked sensitive information of over 3 billion user accounts, exposing them to identity theft. The company had to force all affected users to change passwords and re-encrypt their credentials. In recent years, there have been several instances of such security breaches that have left users vulnerable.

"Almost everything we do on the internet is encrypted for security. The strength of this encryption depends on the quality of random number generation," says Nithin Abraham, a Ph.D. student at the Department of Electrical Communication Engineering (ECE), Indian Institute of Science (IISc). Abraham is a part of a team led by Kausik Majumdar, Associate Professor at ECE, which has developed a record-breaking true random number generator (TRNG), which can improve data encryption and provide improved security for sensitive digital data such as credit card details, passwords and other personal information. The study describing this device has been published in the journal ACS Nano.

Encrypted information can be decoded only by authorized users who have access to a cryptographic "key." But the key needs to be unpredictable and, therefore, randomly generated to resist hacking. Cryptographic keys are typically generated in computers using pseudorandom number generators (PRNGs), which rely on mathematical formulae or pre-programmed tables to produce numbers that appear random but are not. In contrast, a TRNG extracts random numbers from inherently random physical processes, making it more secure.

In IISc's breakthrough TRNG device, random numbers are generated using the random motion of electrons. It consists of an artificial electron trap constructed by stacking atomically-thin layers of materials like black phosphorus and graphene. The current measured from the device increases when an electron is trapped, and decreases when it is released. Since electrons move in and out of the trap in a random manner, the measured current also changes randomly. The timing of this change determines the generated random number. "You cannot predict exactly at what time the electron is going to enter the trap. So, there is an inherent randomness that is embedded in this process," explains Majumdar.

The performance of the device on the standard tests for cryptographic applications designed by the U.S. National Institute of Standards and Technology (NIST) has exceeded Majumdar's own expectations. "When the idea first struck me, I knew it would be a good random number generator, but I didn't expect it to have a record-high min-entropy," he says.

Min-entropy is a parameter used to measure the performance of TRNGs. Its value ranges from 0

(completely predictable) to 1 (completely random). The device from Majumdar's lab showed a record-high min-entropy of 0.98, a significant improvement over previously reported values, which were around 0.89. "Ours is by far the highest reported min-entropy among TRNGs," says Abraham.

The team's electronic TRNG is also more compact than its clunkier counterparts that are based on optical phenomena, says Abraham. "Since our device is purely electronic, millions of such devices can be created on a single chip," adds Majumdar. He and his group plan to improve the device by making it faster and developing a new fabrication process that would enable the mass production of these chips.

4.What Is Quantum Cryptography? A Look at Quantum Threats And Quantum Solutions

by Matt Swayne
https://thequantuminsider.com/2022/05/27/what-is-quantum-cryptography-a-look-at-quantum-threats-and-quantum-solutions/?utm_source=newsletter&utm_medium=email&utm_term=2022-05-29&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+QCI+Acquires+QPhoton+Canada+s+Can+Do+Xanadu+--+And+More+Quantum+News

What is quantum cryptography? The short answer is that quantum cryptography is simply a field that studies how quantum computers could affect the ability to store and secure data.

What is Quantum Cryptography — Background

The computational power of quantum devices is a double-edge sword in the field of cryptography. Quantum computers are both a threat to the current ways we protect data and messages, but the technology also offers a range of solutions, including several theoretical paths to unhackable data storage and transference.

What is Quantum Cryptography — Problem

"We live on the edge because none of the cryptographic systems we use are proven secure in the sense that there's no mathematical proof that these things cannot be broken." — Massachusetts Institute of Technology mathematician Vinod Vaikuntanathan

Current methods to safeguard data, such as the Rivest-Shamir-Adleman algorithm, better known as RSA, use algorithms, usually based on mathematical principles, to encrypt data so only designated parties have access to the information. While these algorithms remain exceedingly difficult for classical computers to crack, the shear computational wizardry of an adequately powered quantum computer could easily break these encryption methods.

This would allow bad actors the opportunity to look over top secret messages that are important to national security, encrypted business statements and even banking and financial transactions.

In other words, the world's entire economic and security system would be at risk.

What is Quantum Cryptography — Solutions

In the strange world of quantum, blessings and curses are evenly balanced and quantum solutions are available to neutralize these quantum threats.

Post-quantum cryptography offers several algorithmic solutions that are thought to be safe against quantum attacks. Essentially, cryptographers are currently creating algorithms to counter quantum computing's power. So far, dozens of these post-quantum cryptographic methods are being investigated.

Another technique to counter potential quantum hackers is the quantum key distribution. As it name suggests quantum key distribution uses quantum technology to generate keys that are shared between parties.

In what some companies are referring to a "entropy-as-a-service," experts theorize that using cloud-based quantum technology to generate truly random numbers that would serve as — in theory — completely unpredictable keys, so unpredictable that it would be impossible for cybercriminals to guess and use to hack into data.

What is Quantum Cryptography — Timeline

The question: What is Quantum Cryptography is usually quickly followed with: When will I need Quantum Cryptography?

The answer is… we don't know for sure. Predictions on when quantum computers will be robust enough to crack current encryption methods range from about lunch time today to lunch time a few decades from now.

No matter what the timeline is, though, cybersecurity experts recommend you prepare for this "when-not-if" scenario today.

In fact, as Duncan Jones, head of Quantinuum's cybersecurity chief points out, today's — and even yesterday's — data is vulnerable to tomorrow's quantum computers: "As soon as we cross this point in time when quantum computers are able to unpick this data, then you would technically be able to read the past like an open book. The question that companies and organizations — particularly governments and the military — need to be asking is: 'Are we sharing something today that will still have value to somebody in ten years time?'"

5.Top 35 Open Source Quantum Computing Tools in 2022

by James Dargan

https://thequantuminsider.com/2022/05/27/quantum-computing-tools/?utm_source=newsletter&utm_medium=email&utm_term=2022-05-29&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+QCI+Acquires+QPhoton+Canada+s+Can+Do+Xanadu+--+And+More+Quantum+News

To do a job properly, you need the right tools for the job—that's a given in area profession you can think of. And in the Quantum Computing (QC) industry is no different. For this emerging sector to grow as a community, one aspect which must develop is in the area of open-source quantum computing tools to allow users to design, for example, quantum algorithms and the like.

With this in mind, The Quantum Insider Data Platform has compiled and curated a list of thirty-five of the best tools around that will give those interested the opportunity to do something great. Both today and tomorrow. Enjoy!

35 Quantum Computing Tools

ProjectQ, Cirq, Q-CTRL Python Open Controls, Quantify, Intel Quantum Simulator, Perceval, Mitaq Tool, Berkeley Quantum Synthesis Toolkit, QCircuits, Yao, Silq, Paddle Quantum, Tequila, Qulacs, staq, Bayesforge, Bluqat, Quantum Programming Studio, Quirk, QuEST, XACC, Quantum++, Quantum Inspire, QuCAT, QuTIP, OpenFermion, TensorFlow Quantum (TFQ), Quipper, QX Simulator, Quantum Algorithm Zoo, ScaffCC, TriQ, Qbsolv from D-Wave, Quantum Computing Playground, Microsoft's LIQUi|>.

Other Quantum Computing Developer Tools

- Microsoft Quantum Development Kit
- IBM Quantum Experience
- Rigetti Forest
- Quantum in the Cloud
- Penny Lane and Strawberry Field from Xanadu
- Raytheon BBN Open Source Software
- PySimulator
- PyQLab

6.The Cornerstone of Cybersecurity - Cryptographic Standards and a 50-Year

Evolution

by Lily Chen and Matthew Scholl
https://www.nist.gov/blogs/cybersecurity-insights/cornerstone-cybersecurity-cryptographic-standards-and-50-year-evolution

In today's connected digital world, cryptographic algorithms are implemented in every device and applied to every link to protect information in transmission and in storage. Over the past 50 years, the use of cryptographic tools has expanded dramatically, from limited environments like ATM encryption to every digital application used today. Throughout this long journey, NIST has played a unique leading role in developing critical cryptographic standards.

Data Encryption Standard (DES)

In the early 1970s, there was little public understanding of cryptography, although most people knew that military and intelligence organizations used special codes or code equipment to communicate. The National Bureau of Standards (NBS), which NIST was formerly called, initiated a program to develop the Data Encryption Standard (DES) in 1973 to protect computer data and to allow for large-scale commercial interoperability. A 64-bit block cipher with 56-bit key, DES was the first public encryption created by the U.S. government. An exhaustive search attack for a DES key takes only 2^{56} operations, which is trivial in today's computing capacity, but in 1977 DES provided sufficient protection for our electronic data. It became the de facto symmetric key standard of the U.S. commercial cryptographic product industry. Federal Information Processing Standard (FIPS) 46, which specifies DES, was published in January 1977.

Advanced Encryption Standard (AES)

Cryptanalysis techniques and the computing power of attackers have steadily advanced during the past half century, demanding a constant transition to cryptographic algorithms with higher levels of security strength. As historian David Kahn noted in The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, "Much of the history of cryptology of this time is a patchwork, a crazy quilt of unrelated items, sprouting, flourishing, withering. . . The story of cryptology during these years is, in other words, exactly the story of mankind."

By the mid-1990s, it was anticipated that the security strength of DES soon would be overtaken by cryptanalysis advancements. Not only had computing capacity tremendously increased since DES was designed, but more sophisticated cryptanalysis techniques, such as differential and linear cryptanalysis methods, had been developed. In 1997, NIST initiated the first world-wide public competition to solicit a 128-bit block cipher with three key length options: 128, 192, and 256 bits. The winner would be named the Advanced Encryption Standard (AES). This open competition enabled NIST to partner with an international community of cryptographers, academic researchers and industry practitioners.

The open partnership with the international community enabled NIST to select an algorithm that rep-

resented the state of the art design for block cipher with a strength to resist different cryptanalysis methods. The AES competition turned a page for NIST cryptographic standards and solidified NISTs position as the world's leader in cryptography. In 2005, when research results challenged the collision resistance property of the hash function SHA-1, the international security community urged NIST to hold another competition for a new family of hash functions. This demonstrated a widespread enthusiasm for participating in the trusted NIST process, an acknowledgement of NIST leadership, and a reliance on NIST to create needed encryption. Working with our stakeholders, NIST then selected the latest family of hash functions, SHA-3, in 2012 and specified these in FIPS 202.

Public-Key Cryptography

Public-key cryptography, invented in 1976, enabled a game-changing breakthrough in the 21st century, allowing different parties to establish keys without a protected channel and enabling the function of digital signatures. With the Internet explosion of the late 1980s, demand skyrocketed for protocols to establish many-to-many secure communications, which cannot rely on a centralized key distribution. In response to this demand, the Internet Engineering Task Force (IETF) deployed public-key cryptography for key establishment and mutual authentication in Internet protocols. The American Banker Association was an early adopter for financial applications.

An American National Standards Institute (ANSI) group called X9 initiated a much-needed standard for public-key cryptography, and NIST actively contributed to these new activities. The major public-key cryptography standards developed in X9 were adopted by NIST in NIST Special Publication (SP) 800-56A and SP 800-56B. The supporting signature schemes standardized by X9, such as RSA and Elliptic Curve Digital Signature Algorithms (ECDSA), were also adopted in FIPS 186

Post-Quantum Cryptography (PQC)

A more dramatic transition lies ahead of us. The public-key cryptography that NIST standardized is based on the hardness of either integer factorization or discrete logarithm problems. Quantum computers, once in full scale, will completely change the hardness assumptions, which are based on classical computers. Today's widely deployed public-key cryptography schemes, such as RSA and ECDSA, will not provide any security protection against quantum computers. Even if they are still far off on the horizon, quantum computers raised a mission call to the NIST cryptographic program. We now face an unprecedented urgency to develop quantum-resistant cryptography standards, a.k.a. post-quantum cryptography (PQC) standards.

NIST started to develop post-quantum cryptography standards in 2016 through an open call for proposals for the new algorithms. The candidate algorithms were submitted by 82 design teams with researchers from 25 countries on 6 continents. In the past 6 years, NIST has led the community to intensively analyze and evaluate these candidates. The candidate pool was narrowed down twice, each time considering security, performance, and many other properties. The selection of algorithms is expected to be announced in the spring of 2022. NIST plans to release the first set of draft PQC standards no later than 2023 for public comments, with the final publication scheduled in 2024.

Migration to PQC and Beyond

Considering that cryptographic standards are the cornerstone of cybersecurity, we must work to assure a smooth migration to our new encryption. The Migration to Post-Quantum Cryptography project, a partnership between the National Cybersecurity Center of Excellence (NCCoE) and industry, aims to ease migration from the current set of public-key cryptographic algorithms to the replacement quantum-resistant algorithms.

NIST has a full cryptographic standards portfolio covering the essential cryptographic primitives (low-level, established cryptographic algorithms often used in developing cryptographic protocols) and guidelines on how to use the primitives in different applications. As the world becomes more digitized every day, cryptographic standards are required not only for protecting against extremely powerful attacks by quantum computers, but also for protecting extremely constrained devices, such as sensors, IoT devices, and RFIDs, and we are developing lightweight cryptography standards for these constrained environments. At the same time, NIST continues work in multiple explorative and research projects to investigate advanced cryptographic tools, such as secure multiparty computation for security and privacy needs in applications like AI and Blockchains.

As we reflect on the journey over the past 50 years, we can trace the evolution of cryptographic standards with the demand for new applications, from code signing for open platforms to pervasive wireless communications. NIST has guided every step of the journey, from DES to AES, from SHA-1 to SHA-2/SHA-3, and from 80-bit security strength parameter set to 112-bit and beyond. The evolution will continue, and we are confident we will continue to lead the way.

7.New QKD Stable Secure Protocol

by Karine
https://thequantumhubs.com/secure-communication-with-light-particles/

Based on the so-called Quantum Key Distribution (QKD), researchers at TU Darmstadt have developed a new, tap-proof communication network.

The new system is used to exchange symmetric keys between parties in order to encrypt messages so that they cannot be read by third parties. In cooperation with Deutsche Telekom, the researchers led by physics professor Thomas Walther succeeded in operating a quantum network that is scalable in terms of the number of users and at the same time robust without the need for trusted nodes. In the future, such systems could protect critical infrastructure from the growing danger of cyberattacks. In addition, tap-proof connections could be installed between different government sites in larger cities.

The system developed by the Darmstadt researchers enables the so-called quantum key exchange, providing several parties in a star-shaped network with a common random number. Individual light quanta, so-called photons, are distributed to users in the communication network in order to calculate the random number and thus the digital key. Due to quantum physical effects, these keys are particularly secure. In this way, communication is particularly highly protected, and existing eavesdropping

attacks can be detected.

So far, such quantum key methods have been technically complex and sensitive to external influences. The system of the Darmstadt group from the Collaborative Research Center CROSSING is based on a special protocol. The system distributes photons from a central source to all users in the network and establishes the security of the quantum keys through the effect of so-called quantum entanglement. This quantum-physical effect produces correlations between two light particles, which are observable even when they are far apart. The property of the partner particle can be predicted by measuring a property of the light particle from a pair.

Polarization is often used as a property, but this is typically disturbed in the glass fibers used for transmission due to environmental influences such as vibrations or small temperature changes. However, the Darmstadt system uses a protocol in which the quantum information is encoded in the phase and arrival time of the photons and is therefore particularly insensitive to such disturbances. For the first time, the group has succeeded in providing a network of users with quantum keys by means of this robust protocol.

The high stability of the transmission and the scalability in principle were successfully demonstrated in a field test together with Deutsche Telekom Technik GmbH. As a next step, the researchers at TU Darmstadt are planning to connect other buildings in the city to their system.

8.QuSecure arrives at the post-quantum cryptography party

by Dan O'Shea
https://www.fierceelectronics.com/electronics/qusecure-arrives-post-quantum-cryptography-party

Everyone is talking about post-quantum cryptography (PQC), the batch of algorithms and related solutions that will be required to head off potential cybersecurity attacks originating from quantum computers.

And by "everyone" we mean the National Institute of Standards and Technology, which is due (actually overdue) to release a list of new PQC encryption standards; the Biden White House; which recently set requirements for federal government agencies to adopt PQC; Congress, not only in the Endless Frontier Act, but also a newer bill from Reps. Ro Khanna, Gerry Connollly and Nancy Mace; and a whole bunch of technology companies looking to address the migration from older encryption techniques like RSA to new PQC solutions.

This group includes firms like Sandbox AQ, which recently was spun off from Google owner Alphabet, and now QuSecure. That San Mateo, California-based firm announced its entry into the PQC sweepstakes earlier this week with what its described as an end-to-end PQC encryption platform that addresses the important-and possibly until now-somewhat overlooked aspect of orchestration.

Skip Sanzeri, who fills multiple roles–founder, COO, chief revenue officer, chairman of the board–at QuSecure, told Fierce Electronics, "A lot of companies have point solutions that solve a piece of the problem, but we feel enterprise and government need a full orchestration layer which allows them to do full management and policy management. That's our easy button for navigating this post-quantum environment."

The company's QuProtect offering uses an end-to-end quantum security as-a-service (QSaaS) architecture that combines Zero Trust security and PQC, as well as "quantum-strength keys, high availability, easy deployment, and active defense into a comprehensive and interoperable cybersecurity suite. The end-to-end approach is designed around the entire data lifecycle as data is stored, communicated, and used," according to a QuSecure statement.

Sanzeri added, "We are able to secure any endpoint and create a quantum channel with encryption that is post-quantum. We can't do a rip-and-replace. It's not like an enterprise can just tear out a bunch of stuff like it's Legos. So we built a protocol switch which allows us to be backwards compatible, and that means that we can translate between a quantum layer and a TLS [transport layer security] layer really, really easily. And that means that enterprises can do this at their pace."

QuSecure is coming out of the gate already touting relationships with customers such as Franklin Templeton and the U.S. Department of Defense, with which it has several projects. As a way of illustrating how quickly some organization are moving to adopt quantum-resistant cryptography, Sanzeri said QuSecure in recent weeks signed on a "billon-dollar company" as a customer "in three days," and already is starting on the project.

The only challenge with PQC is that the goalposts may move when NIST announces its PQC standards. That announcement has been expected for weeks by many in the quantum sector. Security companies for now are either offering their own flavors of quantum-resistant solutions, or the standard-candidate algorithms, or perhaps both. The final list of standards is in question because at least one of them was successfully hacked by an IBM team evaluating it, but Sanzeri said that standards are a key gating factor to the market opportunity.

"We have to support them because no government agency or large enterprise is going to adopt post quantum cybersecurity without using these standards," he said. "So if anybody's operating outside of that, developing algorithms that aren't approved by NIST, I think it's largely a waste of time. But that's why we built in what we call crypto agility. So we already built all these finalists into our system so it won't matter which ones are approved. We can install all of them and use all of them."

9.Memristor-based PUF for lightweight cryptographic randomness

by Hebatallah M. Ibrahim, Heba Abunahla, Baker Mohammad & Hoda AlKhzaimi
https://www.nature.com/articles/s41598-022-11240-6

Physical unclonable functions (PUF) are cryptographic primitives employed to generate true and intrinsic randomness which is critical for cryptographic and secure applications. Thus, the PUF output (response) has properties that can be utilized in building a true random number generator (TRNG) for security applications. The most popular PUF architectures are transistor-based and they focus on exploiting the uncontrollable process variations in conventional CMOS fabrication technology. Recent development in emerging technology such as memristor-based models provides an opportunity to achieve a robust and lightweight PUF architecture. Memristor-based PUF has proven to be more resilient to attacks such as hardware reverse engineering attacks. In this paper, we design a lightweight and low-cost memristor PUF and verify it against cryptographic randomness tests achieving a unique, reliable, irreversible random sequence output. The current research demonstrates the architecture of a low-cost, high endurance $Cu/HfO_2/p^{++}$ Si memristor-based PUF (MR-PUF) which is compatible with advanced CMOS technologies. This paper explores the 15 NIST cryptographic randomness tests that have been applied to our $Cu/HfO_2/p^{++}$ Si MR-PUF. Moreover, security properties such as uniformity, uniqueness, and repeatability of our MR-PUF have been tested in this paper and validated. Additionally, this paper explores the applicability of our MR-PUF on block ciphers to improve the randomness achieved within the encryption process. Our MR-PUF has been used on block ciphers to construct a TRNG cipher block that successfully passed the NIST tests. Additionally, this paper investigated MR-PUF within a new authenticated key exchange and mutual authentication protocol between the head-end system (HES) and smart meters (SM)s in an advanced metering infrastructure (AMI) for smart-grids. The authenticated key exchange protocol utilized within the AMI was verified in this paper to meet the essential security when it comes to randomness by successfully passing the NIST tests without a post-processing algorithm.

10.Quantum Key Distribution for a Post-Quantum World

by Lee Sattler and Venkata Josyula
https://www.darkreading.com/edge-articles/quantum-key-distribution-for-a-post-quantum-world

New versions of QKD use separate wavelengths on the same fiber, improving cost and efficiency, but distance is still a challenge.

The emergence of quantum computing and its ability to solve computations with incredible speed by harnessing the fundamental properties of quantum mechanics could revolutionize our world. But what does this quantum future mean for data security?

As quantum computing evolves from the test lab to the real world, this unprecedented new form of computing power has massive implications for current forms of encryption and public-key cryptography (PKC), such as Rivest–Shamir–Aleman (RSA) and elliptic curve cryptography (ECC). Against the processing capabilities of quantum computing, which can analyze vast sets of data orders of magnitude faster than current digital computers, these forms of encryption will essentially become vulnerable to bad actors.

In the coming post-quantum future, cryptography solutions built on the rules of quantum physics are essential to ensure that sensitive digital information is distributed safely and securely across the forthcoming quantum Internet. One of the pillars of this more secure quantum computing future is called quantum key distribution (QKD), which uses basic properties of physics to derive encryption keys for secure encryption between two locations simultaneously.

Tapping the Power of Photons

At the physical level, the data bits sent during key exchanges for today's common encryption techniques, such as RSA and ECC, are encoded using large pulses of photons or changes in voltages. With QKD, everything is encoded on a single photon, relying on quantum mechanical properties that allow detection and prevent successful eavesdropping. Quantum objects exist in a state of superposition where the value for a property of the object can be described as a set of probabilities for different values.

The transmission of the encoded photons occurs over what's known as the quantum channel. A separate channel, referred to as the classical channel, established between the two endpoints handles clock synchronization, key sifting, or other data exchange; this channel could be any conventional data communication channel.

Multiple Varieties of QKD

A number of implementations and protocols for QKD are emerging as the technology evolves. For example, discrete variable QKD (DV-QKD) is used in many commercial QKD systems today. A DV-QKD system consists of two endpoints: a sender and a receiver. The quantum connection between these endpoints could be free space or dark fiber. In this case, the sender encodes a bit value, 0 or 1, on a single photon by controlling the phase or polarization of the photon. A separate data connection between the two endpoints is used to communicate information about the quantum measurements and timing.

While initial QKD implementations consisted of separate dedicated fibers for the quantum and data channels, new versions can use separate wavelengths for each channel on the same fiber, leading to more cost-effective deployments and efficiencies.

Other implementations include continuous variable QKD (CV-QKD) and entanglement. With CV-QKD, the sender applies a random source of data to modulate the position and momentum quantum states of the transmission. Entanglement QKD, meanwhile, leverages quantum phenomena where two quantum particles are generated in a way in which they share quantum properties; no matter how far apart they may later separate, a measurement of a property on each will result in the same values.

Challenges Ahead for QKD

Distance remains a constraint on implementing QKD over fiber because the individual photons being transmitted will be absorbed over distance. The laser strength is attenuated to create the individual

photons, and standard telecom equipment cannot be used to repeat or strengthen the signal. In general, between 60 miles and 90 miles is the practical limit.

Methods to extend the distance include trusted exchange, twin field QKD, and quantum repeaters.

- Trusted exchanges act as a repeater — receiving the optical signals, converting them to digital, and then converting them back to optical. Trusted exchanges must be secured to prevent an intruder from reading the transmission while it is in digital form.

- Twin field QKD adds a midpoint node that receives signals from both endpoint nodes, increasing the distance between endpoints to potentially hundreds of miles.

- Quantum repeaters could eventually break the distance barriers of QKD over fiber, providing a function similar to repeaters in telecommunications today: to amplify or regenerate data signals so they can be transferred from one terminal to another.

Advancements in single photon sources and low-noise detectors will further improve the viable distances for QKD.

What's Next for QKD

QKD has significant value in a quantum world due to its ability to enable symmetric key sharing between endpoints and identify when eavesdropping on the quantum channel is occurring. Before it can be broadly implemented by carriers, however, QKD must be supportable in a carrier environment, providing the availability and reliability their customers expect.

For example, disruption of the quantum channel can result in the loss of real-time key material; however, having a secure key storage associated with QKD allows key material to continue to be distributed while investigation of quantum channel outage is occurring. This also means that approaches and capabilities to troubleshoot and manage QKD equipment and services must be developed.

Since QKD relies on quantum mechanics, the observing state will impact the quantum system, and this in itself poses challenges to troubleshooting and management. As the technology continues to evolve and improve, QKD implementations on smaller mobile devices such as drones may eventually become possible. No matter how QKD evolves, it looks to be a promising solution for securing communications on the quantum Internet.

11.The quantum menace: Quantum computing and cryptography

by Matthew Tyson

https://www.infoworld.com/article/3659837/the-quantum-menace-quantum-computing-and-cryptogra-

phy.html

No one knows when, but crypto-menacing quantum machines are coming. Here's how researchers use quantum mechanics to crack large integers in asymmetric cryptography.

Quantum computing continues to inhabit the nebulous space between practical application and theoretical speculation, but it is edging closer toward real-world use. One of the more interesting use cases for quantum computers is modern internet cryptography.

Quantum computing and qubits

Quantum computing's name comes from the fact that it relies on the properties of subatomic particles, governed by laws that seem strange to those of us rooted in the macro world. In particular, quantum computers use qubits instead of the binary digits we know from traditional computer systems.

Qubits are probabilistic in nature, whereas bits are deterministic. A bit ultimately resolves down to a physical switch—albeit one that is very tiny, measured in a handful of nanometers. Bits are binary: either on or off, true or false, 0 or 1.

Not so with qubits.

A qubit's physical basis can be numerous phenomena, like the spin of an electron or the polarization of photons. This is a fascinating topic: the realm of linear equations that bridge imagination and reality. Quantum mechanics is considered an interpretation of an underlying reality, rather than a description, and is home to intense computational complexity.

A qubit's state is described as a linear superposition of the two possible states. Once observed, the state is resolved to true or false. However, the same input will not necessarily resolve to the same output, and the state when unobserved can only be described in probabilistic terms.

From a classical physics standpoint, what is even more astonishing is that qubits in a quantum computer can inhabit multiple states simultaneously. When a computer samples a qubit for its state, it resolves into a single either/or (known as a wave function collapse).

Quantum computing in cryptography

All of this is rather interesting from a scientific and philosophical standpoint. For example, the functionality of quantum computers verifies the effect of observation on particles and suggests that, indeed, God does play dice with the universe. But here, we are concerned with the practical aspects of quantum computing's increasing capacity on our everyday lives. In the coming years, the most profound impact will likely be in cryptography.

The best-known avenue from quantum computing to cryptography is a theoretical breakthrough that occurred in 1994: Shor's algorithm. In theory, this algorithm showed the capacity of a quantum Tur-

ing machine to efficiently solve a class of problems that were intractable using traditional computers: the factoring of large integers.

If you are familiar with asymmetric cryptosystem algorithms like Diffie-Hellman and RSA, you know that they rely on the difficulty of solving factors for large numbers. But what happens if quantum computing solves that?

Cracking large integers with quantum mechanics

Shor's algorithm and a handful of other algorithms leverage quantum mechanics to crack the one-way functions at the heart of asymmetric cryptography. The Adiabatic quantum computation has also been used to attack factorization.

Shor's and other algorithms count on the quantum computer's ability to inhabit a multitude of states by virtue of qubits. They then sample those qubits (which collapses their state) in a way that allows for a high degree of probability in the sampling. Essentially, we hand off the question of "What are the factors for a given number" to the mysterious world of the unseen, where the particle properties can exist in multiple states. Then, we query those properties for the most probable answer. (Yes, this actually works.)

The largest number yet factored by Shor's algorithm is 21. The Adiabatic quantum computation has successfully factored 143.

These algorithms are sophisticated and impressive, but so far, their numbers are paltry. The current standard for RSA is 2048 bits, which is 617 digits! However, while attacking the number 143, researchers unknowingly revealed an approach that allows larger numbers, at least in theory. One example is 56,153, which is still a relatively small number compared to what would be required to compromise real-world cryptosystems. It also depends on a reductive trick that can't be used for all numbers.

The threat to web security infrastructure

What we know for now is that fundamental aspects of the quantum attack on asymmetric algorithms are being ironed out. How fast will the technology advance to the point where it can approach significantly larger numbers?

Interestingly, the symmetric algorithms we use every day (like AES) are not terribly vulnerable to quantum algorithms. Grover's algorithm is the one that applies. It is unable, even in theory, to reduce the time needed to attack these algorithms much further than classic algorithms, provided 256-bit keys are used.

Most symmetrical secured communication, however, establishes its keys via asymmetric exchange. So, most web traffic today is vulnerable to advanced quantum computing attacks. If an attacker can discover the key established at the outset of an interaction, no amount of symmetric encryption will be of use.

So the threat to web security infrastructure is real. Let's think a moment about the dynamics at play. The first things to consider are sheer economics and access. Right now, only organizations awash in cash can afford to tinker with such things. IBM, Google, and research scientists in China are vying for leadership in producing viable systems, along with a host of university efforts. Behind the scenes, government agencies like the US National Security Agency are surely not idle. In fact, NSA has its own take on the issue of public cryptography and quantum computing.

Evolving security for quantum computing

It's unlikely that small scale actors will achieve quantum computing capabilities sufficient to attack modern asymmetric keys until long after large institutions have done it. That means we are in a long period of time where security infrastructure can evolve responsively to the dynamics of quantum computing.

No one knows when truly crypto-menacing quantum machines will emerge, but it seems likely that it will happen. Two yardsticks for getting a handle on the question are the number of qubits in a system and the longevity of those qubits.

Qubits are subject to what is called decoherence. Entropy is always whisking away the delicate ensembles of electrons and photons. The trouble is that both the number and longevity of qubits are tough to quantify. How many qubits are needed for a practical reproducible attack on an RSA 2048 key? Some say dozens, some say millions. How much coherence is required? Some say hundreds of nanoseconds, some say minutes.

And all of this can be upended by techniques like the aforementioned tricky use of pre-processing algorithms. Who knows what ingenious undergraduate is right now thinking up a new approach. The people who factored 143 on a quantum machine didn't even realize they had also cracked 56,153 until two years later.

Post-quantum cryptography

All roads lead to a post-quantum world, and many people are already hard at work on it. The US National Institute of Standards and Technology is hosting competitions for developing quantum-resistant algorithms right now. Some of these efforts are netting results.

In the final analysis, we can say the quantum menace to cryptography is real, based on increasingly more real-world results. But for now, it's more than counterbalanced by countervailing forces. We may eventually have to say goodbye to some of our old beloved algorithms, but new ones will take their place.

It will be an interesting dance to watch over the next decade.

12.The 2022 Gödel Prize

https://eatcs.org/index.php/component/content/article/1-news/2917-2022-05-21-20-13-45?fbclid=IwAR1A0e-ViwhH_y1DDIoZbAF8ESbrhX0RzswFNm8EpJapIwT1py4SSM_f6-M

The 2022 Gödel Prize is awarded to the following papers

- Zvika Brakerski, Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011: 97-106. SIAM Journal of Computing 43(2): 831-871 (2014)

- vika Brakerski, Craig Gentry, Vinod Vaikuntanathan: (Leveled) fully homomorphic encryption without bootstrapping. ITCS 2012: 309-325. ACM Transactions on Computation Theory 6(3): 13:1-13:36 (2014)

The above papers made transformative contributions to cryptography by constructing efficient fully homomorphic encryption (FHE) schemes.

In an FHE scheme, data is securely encrypted as in a standard encryption scheme. In addition, FHE provides capability to compute on the encrypted data and generate encrypted results, without decrypting or requiring any secret key. Such capability unlocks a vast array of applications that let us securely outsource expensive computations to untrusted servers, and securely perform collaborative computations among multiple entities. The notion of fully homomorphic encryption was conceived (as "privacy homomorphisms") in work by Rivest, Adleman and Dertouzos in 1978. Constructing an FHE scheme which enables arbitrary computations on encrypted data, however, remained an open question for the following three decades.

Prior to these papers, one of the authors, Craig Gentry, had presented (in proceedings form only) a construction of FHE in 2009. That groundbreaking contribution had great promise, but also some limitations, regarding both efficiency and the nature of the security guarantees. The above papers presented entirely new constructions of fully homomorphic encryption whose security relied only on the hardness of Regev's learning with errors (LWE) problem. They have led to a new generation of practically efficient FHE.

These papers have had enormous impact on both theoretical and applied research, ranging from the constructions of advanced cryptographic primitives, via worst-case to average-case reductions, to FHE implementation, and the design of post-quantum encryption candidates.

13.Protecting data now as the quantum era approaches

by Jeff Burt
https://www.theregister.com/2022/05/20/quantum-security-qusecure/

Startup QuSecure will this week introduce a service aimed at addressing how to safeguard cybersecurity once quantum computing renders current public key encryption technologies vulnerable.

It's unclear when quantum computers will easily crack classical crypto – estimates range from three to five years to never – but conventional wisdom is that now's the time to start preparing to ensure data remains encrypted.

A growing list of established vendors like IBM and Google and smaller startups – Quantum Xchange and Quantinuum, among others – have worked on this for several years. QuSecure, which is launching this week after three years in stealth mode, will offer a fully managed service approach with QuProtect, which is designed to not only secure data now against conventional threats but also against future attacks from nation-states and bad actors leveraging quantum systems.

"The current and near-term capability in quantum computing, which would allow for the decryption, is the big threat," Mike Brown, a retired Navy rear admiral and former senior cybersecurity specialist with the Department of Defense (DoD) and Homeland Security (DHS), told The Register. "That's what we've been talking about for years."

Brown, founder and president of security consultancy Spinnaker Security, who now onsults with QuSecure and other companies, said there has been steady progress in building up the capabilities of quantum computers in the US and abroad. He points out that nation-states with a checkered history in cyberspace, such as China, are spending huge sums and mounting massive efforts to develop such systems.

Steal now, decrypt later

A key worry is what is known as "steal now, decrypt later," QuSecure co-founder and COO Skip Sanzeri told The Register.

"This is the biggest problem, where data gets exfiltrated and it sits on servers waiting to be decrypted. If that data has 50 or 75 years of life left in its value [and] you crack it in 10 years, that's 40 to 65 years of value. This is the problem," Sanzeri said.

"This is why things need to happen. We're getting a lot of inbound inquiries from both federal and commercial [entities]. We've got pilots going across both sides of it. People are now starting to take it seriously."

The Biden Administration earlier this month issued a national security memorandum to address quantum computing and security, including ordering federal agencies to begin a multi-year process of migrating computer systems to quantum-resistant cryptography.

In addition, a bipartisan bill – dubbed the Endless Frontiers Act – calls for spending $100 billion on emerging technologies, including quantum computing and artificial intelligence, to close the innovation gap with China. The bill is moving through Congress.

Another bill, the Quantum Computing Cybersecurity Preparedness Act, is also finding bipartisan support to ensure that government systems adopt post-quantum cryptography by securing systems with algorithms and encryption that will be difficult for even quantum computers to break.

The USA's National Institute of Standards and Technology (NIST) is undergoing a multi-year process of setting such standards, with the hopes of publishing those by 2024.

The promise of quantum

Quantum computers promise to solve problems that are out of reach of today's supercomputers.

Classical computing elements are bits, which can be either 0 or 1. Quantum computing uses qubits, can be 0, 1 or any combination – what's referred to as a superposition. The concern is quantum systems will easily be able to break encryption methods that would take the most powerful machines today years to crack.

Like other vendors, QuSecure is working to address these challenges. It's QuProtect as-a-service architecture includes a software suite that combines zero-trust, post-quantum cryptography, quantum-strength keys and active defense. It leverages Quantum Random Number Generation (QRNG) to create truer randomness in the encryption keys, which is central to secure encryption because patterns in keys can often be detected by cryptanalysts.

The architecture also relies on a proprietary technique that enables QuSecure to get this protection out to the various endpoints, from on-premises servers and web browsers to the Internet of Things and the edge, while also ensuring the security of the networks that data traverses.

"We now have a way to create a quantum channel without putting software out on all these devices," Sanzeri said. "This method that we've discovered and are using … allows us to create quantum channels rapidly between any end devices. If you think of IoT and edge, a lot of time those little sensors don't have any storage capacity, almost no compute capacity aside from doing the one job they do. But we can still secure those."

That said, if an enterprise or government agency needed to keep its data behind a firewall, QuSecure will manage it on-premises or in a private cloud.

QuSecure also built software interfaces, a UI and protocol switch and developed the ability to send encryption keys. It also partners with companies like Quintessence Labs and ID Quantique for QRNG.

In addition, it has what Sanzeri called "crypto agility." The architecture is optimized for all the algorithm finalists in the NIST program, so it doesn't matter which ones the organization eventually chooses, it will be supported by the QuSecure service.

14.Next-Generation Cryptography: How to Secure Your Data Like Never Before

by Shaun Mc Brearty

https://www.toolbox.com/tech/innovation/guest-article/next-generation-cryptography-how-to-secure-your-data-like-never-before/

Cryptography is an essential aspect of modern cybersecurity, but misconceptions about its capabilities abound. Shaun McBrearty, co-founder of Vaultree, discusses overcoming these misconceptions by learning about next-gen encryption and securing your data with maximum protection. Data breaches continue to occur despite increased security efforts and are getting more costly. According to the 2021 IBM Cost of a Data Breach study, the average cost of a data breach increased 10% to $4.24 million, setting a new high since the yearly report began. However, if the information exposed in a data breach is encrypted, hostile actors will be unable to use it. Cryptography is effectively an internal barrier, so your business is still protected even if the outward barrier is breached. When it comes to security solutions, however, most attempts still have a reactive rather than proactive focus. Although cryptography and encryption have numerous benefits, adoption is still limited, owing to a number of residual misconceptions. Let's look at those misconceptions and how cryptography fits into the modern organization, and how to put it in place.

What Is Cryptography All About?

Encryption is the process of transforming information into unreadable text so that it can be stored or transmitted safely. Text messages sent using mobile apps such as WhatsApp are one example. Users can generally find a statement within the app stating that it enables end-to-end encryption. This means that each communication you send gets jumbled and transformed into incomprehensible data. The communication is encrypted as it leaves the app (on one end) and is unscrambled when it reaches the receiver. The information is only readable again at the recipient's end. This procedure prohibits a third party from seeing what was transmitted. This is a well-functioning system. Though current cryptography uses algorithms, advanced math and computer science, the essential premise remains the same: convert information into something that only those with the correct "key" can decipher. One of the most basic methods for ensuring your company's security is encryption. It ensures that, even if your servers and computers are attacked or if information is leaked due to human error, third parties will not be able to read it.

Barriers to Encryption Adoption

But why aren't encryption and cryptography used more frequently if they function so well? For starters, education about cryptography needs to become more common. Typically, cryptographers have a background in mathematics. It takes a lot of knowledge for software engineers to employ encryption. For developers, the cryptographer solutions are very technical, but cryptography addresses so many problems in software development that it's worth the effort to provide more information to developers. In addition, scalability is seen as a problem. There's a popular belief that while working with huge volumes of data, your performance will be constrained as the volume of data grows. Finally, many people believe cryptography is slow – and many of these algorithms are. So, once again, there is apprehension regarding performance. And many individuals wrongly believe that you can't operate with fully encrypted data since it must first be decrypted.

Next-gen Cryptography

Cryptography's perceived complexity is holding it back from widespread usage, but it doesn't have to be that way. Cryptography can be boiled down to a simple method that doesn't cause software developers any additional headaches. Some of today's new technologies are designed to be much more plug-and-play for developers. You don't have to choose between speed and performance when adopting encryption. Cryptography is a powerful technique that may be applied to various situations. It can be applied to several layers of the database. **Full disk encryption, column-level encryption and row-level encryption** are all possible options. There are numerous approaches to choose from. Some methods for setting up a particular configuration are one-touch, while others involve a lot more human effort, and there are various security levels available. True, many outdated systems require certain performance sacrifices to achieve the necessary level of security – but this is changing with the development of new and more advanced encryption methods. Although the notion persists that you can't work with fully encrypted data, things continue to advance and change in this developing field. Technology has progressed to the point where you can now safely process data. There's a misperception that fully homomorphic encryption is slow since it allows calculations on data while it's encrypted, but this isn't necessarily the case. Significant progress is occurring on this front.

The Journey Begins

Data breaches aren't going to stop happening suddenly, and the expense of defending against them is increasing. Cryptography's beauty lies in its ability to make data breaches almost insignificant because criminals can't make sense of what they've stolen – it's meaningless to them. Deploying cryptography may seem complicated, but it doesn't have to be. Next-generation cryptography corrects the most common misunderstandings people have and provides greater data security. Some solutions are ready to connect to your system and have numerous deployment options. Take all of the information noted above into consideration as you begin your encryption journey.

15.Xiphera's new IP cores complement the existing ECC portfolio

https://www.design-reuse.com/news/51974/xiphera-elliptic-curve-cryptography-ecc-ip-cores.html

Xiphera expands its **Elliptic Curve Cryptography (ECC) portfolio** with two new IP cores: **XIP4123C** and **XIP4133C** (together referred as XIP41x3C). Both of these IP cores support Elliptic Curve Diffie-Hellman (ECDH) key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) digital signatures. XIP4123C implements them on the NIST (National Institute of Standards and Technology) P-256 elliptic curve and XIP4133C on the NIST P-384 curve defined by in FIPS PUB 186-2, 186-3, 186-4, and 186-5. These two curves are arguably the most widely-used elliptic curves nowadays and, therefore, the XIP41x3C IP cores complement Xiphera's existing ECC IP cores that support X25519 key exchange and Ed25519 digital signatures.

XIP41x3C family of IP cores are versatile IP cores that have applications in several cryptographic

protocols and systems. ECC on NIST P-256 and/or P-384 is used, for example, in TLS 1.2 and TLS 1.3, IPsec IKEv2, and numerous other protocols. The world of asymmetric cryptography is experiencing a major change in the coming years when Post-Quantum Cryptography (PQC) is being adopted. Despite the emergence of PQC, also ECC has an important role to play in the future in hybrid systems combining PQC and ECC. These hybrid systems will provide security against attacks even in the case if weaknesses are found from the new PQC cryptosystems. In Xiphera's next webinar, The Role of Elliptic Curve Cryptography in the Post-Quantum Era, we will discuss this topic at a deeper level. Register now for free!

The resource footprint of XIP41x3C cores has been carefully optimised and they require only about 1000 6-input LUTs, 1-2 hardwired multiplier(s), and a few embedded memory blocks on a typical modern FPGA device. These impressively small numbers allow our customers to integrate ECC functionalities even in congested designs in small FPGA devices. Despite the small resource usage, XIP41x3C can still perform several cryptographic operations in one second: for example, one ECC key generation takes 21.5 ms on NIST P-256 when XIP4123C is clocked at 200 MHz. This level of performance is sufficient for most ECC use cases, for example, in industrial automation or highly secure systems.

Various features for improved security

XIP41x3C cores include many features that guarantee secure design of the systems. As an example, there are two different interfaces so that only one of them has access to the secret values used in ECDH and ECDSA. This allows, for example, to design systems where XIP41x3C can be used for signing documents without the signer having access to the secret signing keys. XIP41x3C also have a strong level of protection against side-channel attacks. In particular they have fully constant latencies for all operations that use the private keys and they are fully protected against all timing attacks as a consequence.

"ECC has become the de facto standard for implementing asymmetric cryptography during the last decades and the NIST prime curves are the most widely-adopted ways to implement ECC. Although new PQC will be taken into use in the coming years, ECC will still be important for years to come and this is why we at Xiphera decided that it is important to extend our ECC portfolio with efficient and – most importantly – very secure IP cores for ECC on NIST prime curves", says Kimmo Järvinen, Co-founder and CTO of Xiphera.

16.Quantum computing just might save the planet

by Peter Cooper, Philipp Ernst, Dieter Kiewell, and Dickon Pinner
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/quantum-computing-just-might-save-the-planet

The emerging technology of quantum computing could revolutionize the fight against climate change,

transforming the economics of decarbonization and becoming a major factor in limiting global warming to the target temperature of 1.5°C.

Even though the technology is in the early stages of development—experts estimate the first generation of fault-tolerant quantum computing[1] will arrive in the second half of this decade—breakthroughs are accelerating, investment dollars are pouring in, and start-ups are proliferating[2]. Major tech companies have already developed small, so-called noisy intermediate-scale quantum (NISQ) machines, though these aren't capable of performing the type of calculations that fully capable quantum computers are expected to perform.

Countries and corporates set ambitious new targets for reducing emissions at the 2021 United Nations Climate Change Conference (COP26). Those goals, if fully met, would represent an extraordinary annual investment of $4 trillion by 2030, the largest reallocation of capital in human history. But the measures would only reduce warming to between 1.7°C and 1.8°C by 2050, far short of the 1.5°C level believed necessary to avoid catastrophic, runaway climate change.

Meeting the goal of net-zero emissions that countries and some industries have committed to won't be possible without huge advances in climate technology that aren't achievable today. Even the most powerful supercomputers available now are not able to solve some of these problems. Quantum computing could be a game changer in those areas. In all, we think quantum computing could help develop climate technologies able to abate carbon on the order of 7 gigatons a year of additional CO2 impact by 2035, with the potential to bring the world in line with the 1.5°C target.

Quantum computing could help reduce emissions in some of the most challenging or emissions-intensive areas, such as agriculture or direct-air capture, and could accelerate improvements in technologies required at great scale, such as solar panels or batteries. This article offers a look at some of the breakthroughs the technology could permit and attempts to quantify the impact of leveraging quantum-computer technology that are expected become available this decade.

Solving so far insoluble problems

Quantum computing could bring about step changes throughout the economy that would have a huge impact on carbon abatement and carbon removal, including by helping to solve persistent sustainability problems such as curbing methane produced by agriculture, making the production of cement emissions-free, improving electric batteries for vehicles, developing significantly better renewable solar technology, finding a faster way to bring down the cost of hydrogen to make it a viable alternative to fossil fuels, and using green ammonia as a fuel and a fertilizer.

Addressing the five areas designated in the Climate Math Report as key for decarbonization, we have identified quantum-computing use cases that can pave the way to a net-zero economy. We project

[1] Fault-tolerant quantum computing, in contrast to NISQ, enables sizable quantum computers to use error correction and perform billions more gate operations, which are necessary for most known valuable algorithms. NISQ-era quantum computers have 50 to several hundred qubits, which is not sufficient for error correction, restricting in the number of gate operations. Currently no valuable NISQ algorithms are known.

[2] The quantum technology monitor, McKinsey, September 2021.

that by 2035 the use cases listed below could make it possible to eliminate more than 7 gigatons of CO2 equivalent (CO2e) from the atmosphere a year, compared with the current trajectory, or in aggregate more than 150 gigatons over the next 30 years.

.
.
.

17.IonQ and Rigetti Discuss their Roadmap Plans

https://quantumcomputingreport.com/ionq-and-rigetti-discuss-their-roadmap-plans/

In their Q1 Finance Results press releases and also during the Q1 calls, both IonQ and Rigetti discussed their roadmap plans for future processors. Peter Chapman, CEO of IonQ, mentioned that the company is currently working on three different generations of processors in different stages of development. The latest released version is called Aria which can hold up to 32 qubits. It is currently available in IonQ's own cloud system and will also be available on Microsoft's Azure system soon. The next version to be released is codenamed Forte which won't have a much larger number of qubits than its predecessor Aria but will have lower noise and improved fidelity. It will also pioneer a new approach for controlling the laser that manipulates the qubits using a technology called Acousto-Optic Deflector (AOD).

The current Aria processor uses a light modulator to control individual laser beams for control while the Forte will use the Acousto-Optic Deflector. It will be software controlled can precisely aim a laser by deflection to control the desired qubit. This approach provides significant advantages because adjustments such as calibration can be implemented via software instead of mechanically. This approach reduces or eliminates crosstalk problems and can also lead the way for more scaling since a single laser beam can address as many a few hundred different qubits.

One surprise in the announcement was that the Forte processor will still use Yterbium ions like its predecessor. IonQ had previously indicated they are planning to move to use Barium. But apparently, this will not occur until the next generation of processors after Forte. Additional information about IonQ's plans is available in a news release announcing the Forte processor available here and comments from Junsang Kim, IonQ CTO, during the Q1 financial results webcast which you can listen to here.

Rigetti discussed their roadmap for future processors. The latest processor currently available is the 80 qubit Aspen-M which consists of two 40 qubit die which are connected together. Rigetti used this processor as the vehicle to develop their multi-die processors technology. It took them six years to develop and they have more than 20 patents as a result of this effort. The multi-die approach will be a keystone technology for many of Rigetti processors in the future.

But before they build more multi-die processors, they are first developing an improved single chip 84

qubit die to use as the base. The new chip they are developing will have an updated lattice, higher connectivity, and improvements in two qubit gate fidelity and stability. Rigetti plans on releasing an 84 qubit processor in early 2023 using this chip. And then, later in 2023, they plan they plan on creating a multi-die implementation with 336 qubits using four of these chips connected together. In the following years, Rigetti expects to have a 1000+ qubit chip in 2025 and a 4000+ qubit chip around 2027. In their Q1 press release and earnings call, Rigetti highlighted some of the challenges they are facing in their technical developments including higher than anticipated costs for labor, equipment, and system component, market and supply chain conditions, and available working capital. But as we have said before, quantum is a difficult technology and we're sure that many of the processor companies are facing similar issues.

For more on Rigetti's plans, you can read their roadmap comments in the Q1 Financial Results press release located here.

18.Quantum key distribution network accurately measures ground vibration

by Bob Yirka

https://phys.org/news/2022-05-quantum-key-network-accurately-ground.html

A team of researchers affiliated with several institutions in China has found that quantum key distribution (QKD) networks can be used to accurately measure ground vibration. In their paper published in the journal Physical Review Letters, the group describes their implementation of a twin-field, fiber-based QKD network over a distance of 658 km. They also determined that the network could be used as a means for sensing ground vibrations associated with earthquakes or landslides.

QKD networks make use of unique quantum properties of photons to encrypt data sent between communication devices. Because of their quantum properties, such networks are nearly impossible to hack without the system hosts noticing the activity and ceasing transport of messages. Because of this feature, scientists in several countries have been working to improve the technology for widespread use. In this new effort, the researchers developed and installed a twin-field, fiber-based QKD network that takes advantage of the way photons interfere as a means of encrypting data, and were surprised to find that the fiber network could also be used to sense ground vibration.

In their work, the researchers successfully sent encrypted data over a 658-km fiber cable, extending the previous distance record by approximately 100 km. In such a network, fluctuations in the phase of the light passing through the fiber cable must be noticed and corrected by stretching the cable in order for the key distribution to work correctly. Such fluctuations, the researchers noted, typically arise due to ground vibrations.

In their system and others like it, a separate fiber cable is used to lock the frequencies between nodes on the network. The researchers found that the timing information in the second cable can accurately determine, to within approximately 1 kilometer, where along the cable the fluctuation was

created. That suggests that systems such as theirs could also serve as ground vibration sensors, possibly warning of an ongoing earthquake or landslide. Notably, for real-world application, the data transfer rate would have to be improved.

19.How to strengthen cyber security the right way

by Subimal Bhattacharjee
https://indianexpress.com/article/opinion/columns/strengthen-cyber-security-right-way-7920843/

On April 28, the Indian Computer Emergency Response Team (CERT-In) issued "directions" under Section 70-B(6) of the Information Technology Act 2000 (IT Act) relating to information security practices, procedure, prevention, response and reporting of cyber incidents. These directions have brought about a wide-ranging expansion in the scope of obligations of the above requirements compared to the Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013 (Rules). Among the activities in which compliance is sought by service providers, intermediaries, data centres and body corporates are the synchronisation of computer clocks to the network time protocol set at the National Physical Laboratory and National Informatics Centre (NIC), mandatory reporting of all cyber incidents within six hours of noticing or being brought to their notice in the prescribed format, designating point of contact and notifying CERT-In and undertaking to perform such actions for cyber security mitigation when notified by CERT-IN, maintaining all logs of all ICT systems up to 180 days within Indian jurisdiction and for data centres, virtual private network service providers, cloud service providers and virtual private server providers to maintain all records of their users and usage for a minimum of five years.

While the overall thrust towards a robust cyber incident reporting and security regime is prudent, some of the provisions in the absence of clarification from CERT-In have raised concerns amongst industry observers and cyber security experts. For some time now, CERT-IN has been struggling to get information and incident reporting from service providers, intermediaries as well as body corporates as per the rules and its mandate under section 70B(4) of the IT Act. This was impacting its responsibility as a collector, analyser and disseminator of information on cyber incidents as well as coordinating incident responses and emergency measures. So, it took recourse to the directions, which strangely do not differentiate between the scales and nature of the incident. Some cyber incidents are far more common and occur regularly. An organisation might receive hundreds of phishing emails and the effort to notify each would drastically increase their compliance cost. It would also be interesting to know what CERT-In's strategy will be for dealing with commonplace cyber incidents and its own capacity enhancement in terms of handling the compliance sought.

A window of 60 days has been provided before implementation of these compliances begins. Given the scale of the revamp, this might be too short a window. The government must look at the concerns that arise from such directions and work out a realistic time scale. The ugly episode of the Twitter incident around compliance with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, last year is a stark reminder of the pitfalls of rushing in compliances

without factoring in concerns. In this case, there will be multiple companies even from the MSME sector that will take time to set up systems for compliances.

All covered entities also have to mandatorily enable logs and maintain them for 180 days within the Indian jurisdiction. At present, most entities maintain logs for around 30 days, and in order to maintain logs for 180 days, the additional data storage device cost would be huge. Similarly, data centres, virtual private server providers, cloud service providers and virtual private network service providers will need to retain additional information for five years or more after the cancellation or withdrawal of registration. The virtual asset industry too will have to maintain all KYC records and details of all financial transactions for five years. The compliance cost in each case is going to rise substantially.

Many of the entities will have to shift their servers geographically as well as add excess storage capacity. Most importantly, the recruitment of additional manpower for compliance may take far longer. A realistic timeline would be six months, which would allow the entities to effectively migrate to the new regime. The penalty for non-compliance is stiff (including up to one year of imprisonment and monetary fines). But it is also unfair to create unrealistic deadlines for industry.

This is also going to significantly affect organisations that have maintained their servers offshore, although the move is in line with the government's stated objective of localising data storage. But what cannot be denied are privacy concerns. With VPNs and virtual asset wallets being asked to store and share KYC and transaction data, these concerns become evident. VPNs have been successful for corporates as well as individuals because they address privacy concerns. There have been very few instances where these tunnels have been used for criminal activities and support from the providers was not obtained by law enforcement authorities. In the absence of legislative backing for data protection, which has been on the anvil for more than two years, the question is: How will the user have any say on which information can be held back or how his sensitive personal information is being protected?

While CERT-In has been proactive in recognising the changing frontiers of technology and trying to deal with hitherto unknown cyber threats, it is wanting in terms of a graded approach to ensuring compliance.

20.Top 18 Leading Quantum Computing Research Institutions 2022

by Matt Swayne

https://thequantuminsider.com/2022/05/16/the-top-18-research-institutions-leading-the-recent-surge-of-quantum-computing-investigations/

So far, 2022 has been a banner year for quantum computing research. Several quantum-based companies have moved to go public, including at least two announcements of special acquisition companies being created to accommodate interest in quantum. Multinational corporate mergers have also started to happen in the quantum industry.

According to data gathered from Microsoft Academic, several universities and research institutions are consistently producing research papers, conference presentations and other forms of academic output in the quantum computing area. The groups represent both corporate computing research teams and university-based scientists.

We've organized a list of 18 of today's most respected – leading – quantum computing research institutions.

(i) IBM

IBM was mentioned in about 786 pieces of research output so far this year.

IBM quantum research teams and research equipment were involved in the research output including the papers, Quantum Computer Systems for Scientific Discovery, Evidence of the entanglement constraint on wave-particle duality using the IBM Q quantum computer (Physical Review A) and Application of Quantum Machine Learning to High Energy Physics Analysis at LHC using IBM Quantum Computer Simulators and IBM Quantum Computer Hardware, presented at 2021 Proceedings of 40th International Conference on High Energy physics.

Find out more about IBM's quantum efforts here.

(ii) Massachusetts Institute of Technology

Massachusetts Institute of Technology — better known as MIT — is a world-renowned center for science, technology and engineering. MIT has been a pioneering hub for work in quantum.

In 2022, researchers from MIT played roles in major advanced in quantum technology that were published in leading scientific journals, including: Room-temperature photonic logical qubits via second-order nonlinearities, which appeared in Nature Communications; Capturing Non-Markovian Dynamics on Near-Term Quantum Computers, Physical Review Research; and Creating Majorana modes from segmented Fermi surface, again in Nature Communications.

Find out more about quantum information science at MIT here.

(iii) Harvard University

Harvard continually makes lists for various scientific achievements. It is perennially on the top of lists for quantum science. According to Microsoft Academic, this legacy as a global leader in science and quantum research continues in 2022, with more than 1,800 entries in the quantum computer category on the research.

Some of the studies, published both in major scientific journals and pre-print servers, such as ArXiv, that include Harvard researchers are: Quantum Computing lab at the Frontiers of Biological Sciences in Nature Methods; Quantum Information and Algorithms for Correlated Quantum Matter in Chemical Reviews and Quantum Computing and Quantum Information Storage in Physical Chem-

istry Chemical Physics.

Here's more information about Harvard's quantum initiative.

(iv) Max Planck Society

The Max Planck Society, established in 1948, has produced 20 Nobel laureates and is considered one of the world's most prestigious research institutions worldwide. Its scientists are producing cutting-edge research in the fields of quantum computing, as well. This year, MPS is among the leaders in quantum computing research. So far in 2022, Max Planck Society scientists have published "A Auantum-logic Gate Between Distant Quantum-network Modules" in Science and "Topological Two-Dimensional Floquet Lattice on a Single Superconducting Qubit" in Physical Review Letters, among dozens of other published research pieces.

Quantum science at the Max Planck Society is covered here.

(v) University of Chicago

In the U.S. the heartland is also the heart of quantum-land, thanks, in no small part, to the University of Chicago.

In 2022, University of Chicago researchers have taken part in several key quantum computing studies including, "Engineering Dynamical Sweet Spots to Protect Qubits from 1/f Noise," which appeared in Physical Review Applied; "Quantum Solver of Contracted Eigenvalue Equations for Scalable Molecular Simulations on Quantum Computing Devices," published in Physical Review Letters and "Orchestrated trios: compiling for efficient communication in Quantum programs with 3-Qubit gates," which was presented at ASPLOS 2021.

Chicago Quantum Exchange is a great resource for learning more about quantum science at the U of Chicago.

(vi) Chinese Academy of Sciences

The first Chinese entry on the list of top quantum research institutions is a research powerhouse in China. In just a few short months, the Chinese Academy of Sciences has amassed more than a thousand entries.

Most recent entries in that list of quantum computing research advances are "Observation of energy-resolved many-body localization," published in Nature Physics; "A concise review of Rydberg atom based quantum computation and quantum simulation," Chinese Physics B and Solving quantum statistical mechanics with variational autoregressive networks and quantum circuits, which appeared in Machine Learning Science and Technology. They also invested a lot in a development of quantum computing labs.

Read more about the academy's research advances here.

(vii) University of California, Berkeley

The University of California, Berkeley is located in the heart of California's quantum country. Its research output thus far this year — and its solid industrial and government connections — make it a top ten entrant on our list of the most productive research institutions.

Berkeley researchers contributed to published papers include: "Quantum approximate optimization of non-planar graph problems on a planar superconducting processor," in Nature Physics; "Efficient and noise resilient measurements for quantum chemistry on near-term quantum computers," npj Quantum Information and "Materials challenges for trapped-ion quantum computers," Nature Reviews Materials.

Read more about the University of California's quantum advances at Berkeley Quantum.

(viii) University of Maryland, College Park

Home of one of the first quantum computer firms to go public (IonQ) and a constant addition to TQD's "best of" lists, the University of Maryland, College Park is showing no signs of slowing down research output in the quantum computing labs.

UoM research teams participated in the following studies and published papers: "Probing many-body localization on a noisy quantum computer," Physical Review A; "Microwave Superconductivity," IEEE and "Conformal field theories are magical," Physical Review B.

Learn more about the Joint Center of Quantum Information and Computer Science.

(ix) Princeton University

The second Ivy League school in the list of top quantum research institutions is probably a no-brainer, if that term can be used without irony. Princeton has a well-established reputation as being one of the world's centers of academic and research excellence. That reputation continues in quantum.

This year, Princeton researchers have participated in several quantum advances reported in journals and on pre-print servers, including "New material platform for superconducting transmon qubits with coherence times exceeding 0.3 milliseconds," Nature Communications; "Spin Digitizer for High-Fidelity Readout of a Cavity-Coupled Silicon Triple Quantum Dot," Physical Review Applied and "CutQC: using small Quantum computers for large Quantum circuit evaluations," ASPLOS 2021.

Learn more about quantum at Princeton here.

(x) Google Quantum Computer Research Center

From the company that developed the first quantum computer to assert quantum supremacy,

Google researchers continue to make impressive strides in the quantum computing field.

For this year, the company's scientists have taken part in studies, including "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," in Quantum; "High-Fidelity Measurement of a Superconducting Qubit Using an On-Chip Microwave Photon Counter," in Physical Review X and "Power of data in quantum machine learning," in Nature Communications.

Explore the possibilities of quantum with Google.

(xi) University of Tokyo

Japan is a hub of research into technology and information science. This research prowess extends to the quantum era.

The University of Tokyo is home to scientists who took part in the following recent studies and published papers: "Blueprint for a scalable photonic fault-tolerant quantum computer," which appeared in Quantum; "Post-Hartree–Fock method in quantum chemistry for quantum computer," published in European Physical Journal and "Event Classification with Quantum Machine Learning in High-Energy Physics," presented in Computing and Software for Big Science.

Read more about this quantum initiative at the University of Tokyo.

(xii) University of Science and Technology of China

Our second entry to the list from China continues to astound the world with its scientific advances in quantum computing.

Scientists from the University of Science and Technology of China have been involved in quantum computer lab studies, including: "Testing a Quantum Error-Correcting Code on Various Platforms," in Chinese Science Bulletin; "Experimental exploration of five-qubit quantum error correcting code with superconducting qubits," in National Science Review and "Quantum walks on a programmable two-dimensional 62-qubit superconducting processor" in Science.

Here's the Division of Quantum Physics and Quantum Information at USTC.

(xiii) University of Washington

The Seattle-based University of Washington is growing into its role as one of the leaders in quantum science and, in particular, in quantum computing. A recent surge in published research papers about quantum computing include University of Washington researchers leading the charge.

Those projects include: "Sparse-Hamiltonian approach to the time-evolution of molecules on quantum computers,"The European Physical Journal," "Entanglement rearrangement in self-consistent nuclear structure calculations," Physical Review C and "Qubit Regularization of Asymptotic Freedom" in Physical Review Letters.

You can read about one U of W quantum initiative here.

(xiv) University of Oxford

The University of Oxford's contributions to quantum science are legendary. The university is now one of the leaders sherparding the world from classical to Noisy Intermediate Scale Quantum — NISQ — and beyond.

Here are a few projects Oxford scientists are involved in that have implications in quantum computing: "Multi-exponential error extrapolation and combining error mitigation techniques for NISQ applications," which appeared in npj Quantum Information; Non-Gaussianity as a Signature of a Quantum Theory of Gravity, which was published in PRX Quantum and The prospects of quantum computing in computational molecular biology, which appeared in WIREs Computational Molecular Biology.

Here's an example of a quantum computer project at the University of Oxford.

(xv) Duke University

Duke University is probably not a research institution that most immediately associate with quantum computing compared to some of the other institutions. (Duke's research trail only leads back to 1998, while some of the other universities have quantum computing work that originated in the 1980s, even the 1970s...)

But that's changing as the following quantum projects show: "Materials challenges for trapped-ion quantum computers," Nature Reviews Materials; "Optimizing Stabilizer Parities for Improved Logical Qubit Memories," ArXiv and "Practical Applications with Quantum Computers," presented at Quantum West.

As an example of Duke's forward-looking quantum progress, check out this initiative.

(xvi) National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology supports quantum science both in the U.S. and around the world. The soul of NIST's support is in the prowess of its researchers.

Here are a few NIST-backed research projects: "Ray-Based Framework for State Identification in Quantum Dot Devices," PRX Quantum; "Towards data-driven next-generation transmission electron microscopy," Nature Materials and "Control and readout of a superconducting qubit using a photonic link," in Nature.

Read more about NIST's support of quantum in this TQD article.

(xvii) Stanford University

Seated geographically right in the hottest of technological hot spots, Stanford University is among the top research institutions for the high tech world.

In quantum computing, its recent publications show scientists involved in the following projects: "Quantum Permutation Synchronization," in ArXiv; "Recycling qubits in near-term quantum computers," in Physical Review A and "Connecting and scaling semiconductor quantum systems," presented at Photonic and Phononic Properties of Engineered Nanostructures XI

Read about Stanford's Quantum Computing mission here.

(xviii) California Institute of Technology

You can't have Caltech without the tech part and it's rapidly becoming a quantum powerhouse.

Just some of the work done recently by scientists at California Institute of Technology include: Power of data in quantum machine learning, in Nature Communications; "Low rank representations for quantum simulation of electronic structure," in npj Quantum Information and "Quantum Computation of Finite-Temperature Static and Dynamical Properties of Spin Systems Using Quantum Imaginary Time Evolution," in PRX Quantum.

CalTech quantum projects include the Institute for Quantum Information and Matter.

21.Russian hackers declare war on 10 countries after failed Eurovision DDoS attack

by Connor Jones
https://www.itpro.co.uk/security/hacking/367685/russian-hackers-declare-war-on-10-countries-after-failed-eurovision-ddos

Russian-linked hackers have claimed to have disrupted the infrastructure of Italy's State Police anti-cyber crime arm after it thwarted hacking attempts on the Eurovision Song Contest.

Hackers from the Killnet group announced in the early hours of Monday morning that claims made by Italian State Police referred to the disruption of cyber attacks over the weekend were false.

In the same announcement, Killnet also "declared war" on 10 countries, including the "deceitful police of Italy", and appeared to mock the authority, claiming Killnet was responsible for the seemingly off-line website of the police's cyber department.

The website of Italy's anti-cyber crime organisation, Cnaipic, was involved in the prevention of Russian-linked hacking attempts on the Eurovision song contest's voting systems, Italian State Police said, and at the time of writing, its website also appears to be down.

Cnaipic assigned officers to work 24 hours a day in a unit dedicated to protecting Eurovision's infrastructure which was ultimately attacked by the Russian-linked Killnet and Legion hacking groups.

Italian State Police confirmed its response on Sunday, saying they were able to "neutralise and repel the attacks".

"Various computer attacks of a DDoS were nature directed at network infrastructure during the voting operations and the singing performance were mitigated in collaboration with the ICT Rai and Eurovision TV management," said the State Police, as reported by ANSA. "Identified by the Cnaipic of the Postal Police, numerous 'PC-zombies' were used for the cyber attack."

This year's Eurovision Song Contest was held in Turin, Italy and saw Kalush Orchestra from Ukraine was crowned the champion after many predicted the country to win following Russia's invasion.

Authorities said the distributed denial of service (DDoS) attacks were prevented during the competition's grand final and during the final voting stages.

State Police also said they scoured the hacking groups' associated Telegram channels to glean intelligence that led to the prevention of other incidents and the identification of the hackers' location.

Sustained Killnet attacks

Days before the Eurovision Song Contest, Italian authorities reported, via ANSA, that the same Killnet hackers had targeted the websites of the Italian National Health Institute and Automobile Club d'Italia, a national drivers' association.

The Italian senate's website was also targeted in the attack which saw hackers take down web pages for roughly an hour.

Italian senate speaker Elisabetta Casellati said via Twitter that no damage was sustained from the attack on the senate.

"Thanks to the technicians for the immediate intervention," she said. "These are serious episodes, which should not be underestimated. We will continue to keep our guard up."

Killnet has been a group on the watchlist of international cyber crime authorities for some time, with the Five Eyes intelligence alliance previously releasing a joint cyber security advisory naming Killnet as one of the biggest threats to critical infrastructure.

Among other recent attacks, the alliance pointed to a March DDoS attack on Bradley International Airport in Connecticut as previous work carried out by the group which has also released a video pledging support for Russia.

22.The NSA Swears It Has 'No Backdoors' in Next-Gen Encryption

by Lily Hay Newman
https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/nsa-backdoor-encryption-security-roundup/amp

A group of human rights lawyers and investigators called on the Hague this week to bring what would be the first ever "cyber war crimes" charges. The group is urging the International Criminal Court to bring charges against the dangerous and destructive Russian hacking group known as Sandworm, which is run by Russia's military intelligence agency GRU. Meanwhile, activists are working to block Russia from using satellites controlled by the French company Eutelsat to broadcast its state-run propaganda programming.

Researchers released findings this week that thousands of popular websites record data that users type into forms on the site before they hit the Submit button—even if the user closes the page without submitting anything. Google released a report on an in-depth security analysis it conducted with the chipmaker AMD to catch and fix flaws in specialty security processors used in Google Cloud infrastructure. The company also announced a slew of privacy and security features for its new Android 13 mobile operating system along with a vision for making them easier for people to understand and use.

The European Union is considering child protective legislation that would require scanning private chats, potentially undermining end-to-end encryption at a massive scale. Plus, defenders from the cybersecurity nonprofit BIO-ISAC are racing to protect the bioeconomy from digital threats, announcing a partnership this week with Johns Hopkins University Applied Physics Lab that will help fund pay-what-you-can incident response resources.

But wait, there's more. Each week we round up the news that we didn't break or cover in-depth. Click on the headlines to read the full stories. And stay safe out there.

NSA Promises That It Really, Really Didn't Backdoor New Encryption

The United States is completing development of a new generation of high-security encryption standards that will be robust in the current technical climate and are designed to be resistant to circumvention in the age of quantum computing. And while the National Security Agency contributed to the new standards' creation, the agency says it has no special means of undermining the protections. Rob Joyce, the NSA's director of cybersecurity, told Bloomberg this week, "There are no backdoors." The NSA has been implicated in schemes to backdoor encryption before, including in a situation in the early 2010s in which the US removed an NSA-developed algorithm as a federal standard over backdoor concerns.

ICE Surveillance Dragnet Even More Extensive and Well-Funded Than Previously Known

An extensive investigation by Georgetown Law's Center on Privacy & Technology reveals a more detailed picture than ever of US Immigration and Customs Enforcement agency surveillance capabilities and practices. According to the report, published this week, ICE began developing its surveillance infrastructure at the end of the George W. Bush administration, years before it was previously thought to have begun these efforts. And researchers found that ICE spent $2.8 billion on surveillance technology, including face recognition, between 2008 and 2021. ICE was already known for its aggressive and invasive surveillance tactics during the Donald Trump administration's anti-immigration crackdowns, but the report also argues that ICE has "played a key role in the federal government's larger push to amass as much information as possible" about people in the United States.

"Our two-year investigation, including hundreds of Freedom of Information Act requests and a comprehensive review of ICE's contracting and procurement records, reveals that ICE now operates as a domestic surveillance agency," the report says. "By reaching into the digital records of state and local governments and buying databases with billions of data points from private companies, ICE has created a surveillance infrastructure that enables it to pull detailed dossiers on nearly anyone, seemingly at any time."

Clearview AI Agrees Not to Sell Face Rec Database in US

In a legal settlement this week, the face recognition and surveillance startup Clearview AI agreed to a set of restrictions on its business in the US, including that it won't sell its faceprint database to businesses or individuals in the country. The company says it has more than 10 billion faceprints in its arsenal belonging to people around the world and collected through photos found online. The settlement comes after the American Civil Liberties Union accused Clearview of violating the Illinois Biometric Information Privacy Act. The agreement also stipulates that the company won't be allowed to sell access to its database in Illinois for five years. "This settlement demonstrates that strong privacy laws can provide real protections against abuse," Nathan Freed Wessler, a deputy director of the ACLU Speech, Privacy, and Technology Project said in a statement. Despite the privacy win, Clearview may continue to sell its services to federal law enforcement, including ICE, and police departments outside of Illinois.

Costa Rica Declares National State of Emergency After Conti Ransomware Attack

Costa Rican president Rodrigo Chaves said on Sunday (08 May 2022) that the country was declaring a national emergency after the notorious **Conti ransomware** gang infected multiple government agencies with malware last week. Sunday was the first day of Chaves' presidency. Conti leaked some of a 672 GB trove of stolen data from multiple Costa Rican agencies. In April, the Costa Rican social security administration had announced that it was the victim of a Conti attack. "At this time, a perimeter security review is being carried out on the Conti Ransomware, to verify and prevent possible attacks," the agency tweeted at the time.

23.Best Questions to Ask When Picking a New Computer Security Product

by Roger Grimes
https://www.linkedin.com/pulse/best-questions-ask-when-picking-new-computer-security-roger-grimes/

Finding and picking a new computer security defense solution is hard. Well, finding it may not be. We all get besieged by vendors non-stop all the time. They all claim that if you just buy their product, your worries will be gone. Just buy and forget.

There is a lot that goes into figuring out if a particular solution is right for you, including:

- **Functionality**
- **OS Support**
- **Ease-of-Use**
- **Cost: Initial purchase price, installation, ongoing operations and maintenance, etc.**
- **Impact on productivity**

And more.

But to me, the biggest question I need to ask before considering purchasing a product is, how well does it actually prevent the cybercrime that it claims to prevent?

The antivirus world is a great example. There is hardly an antivirus product that does not make some 100% or 99% claim of being able to detect whatever malware that comes your way. They have reams of proof, papers and independent studies backing up how great they really are. 100%! You can believe them, I'm sure.

Except I have never found a single AV product that can detect most of the new malware samples I submit...ever! Even today, I can submit a new malware program to Google's VirusTotal, which currently runs 83 popular antivirus programs, and rarely get a detection hit. All of them usually miss what I am presenting, and I am always presenting real malware that I have verified using my own virtual machines and/or testing. Even after a week or month, the vast majority of them still do not detect the sample. Some of the AV programs seem to detect more legitimate files as malicious than the other way around.

I am sure anyone in the AV industry just hates me right now, but if AV (or even EDR solutions) detected 100% of maliciousness all the time, the world would beat a path to their door, pay a big premium for the product and our malware problems would be over. But nothing like 100% detection exists. In fact, malware attacks have never been more pervasive and successful than now. That is the real fact.

So, how do you know if you are being taken for a ride when a vendor says their product detects 100% of something or can do anything they claim 100% of the time?

Well, make the vendor prove it before you buy it.

Start with declaring the goal of the product. What does it claim to do? What does it claim to prevent? What do you think it will do? Clarify with the vendor that your hopes of what it will mitigate match what it can do. Then document the goal. Success of the test then becomes the product meeting that goal. It is important to do this step because reviewers often get sold on overhyped marketing of what the product might do instead of what the product actually can do. So, get agreement from the vendor about what it is capable of and what it cannot do. This is documenting expectations and understandings.

A good example of this is a claim my employer, KnowBe4, makes. KnowBe4 says any customer using our security awareness training products as recommended (which means at least monthly training and simulated phishing tests) will significantly reduce the percentage of their employees who click on a real (or simulated) phishing attack. We claim that the average organization has about 30% of employees who will click on a standard-looking phishing email/link without training. And after recommended training and testing, that figure goes below five percent.

Try it yourself. Do a "phishing prone" test. Send out a simple, standard-looking, simulated phishing email and see what percentage of participants respond to it. It is probably going to be 30% or higher. OK. Then start to do the recommended testing and training. Did the phish prone rate fall significantly to below five percent or not? If you cannot test, ask for the contact information for customers who did buy and test. Or even better, just ask a friend who is running the product AS RECOMMENDED, to see what they say. Proof is in the pudding...whatever that means.

For most computer security products, you are going to test and develop, various attack scenarios that the product claims to mitigate ahead of time. Figure out how to realistically simulate the various attacks the product claims to mitigate or detect. Document the inputs you will use to accomplish the simulated attacks and expected product outcomes (e.g., detection, mitigation, block, alerting, reports, etc.). Create a broad set of real-world scenarios. The more real-world the better. It is key that you create your own real-world attack scenarios that your organization is likely to be threatened by. Do not let the vendor get involved in this step, or at least the first set of attempts. That is because vendors will always lead you into scenarios where they know their product excels. They will always knock those scenarios out of the ballpark. So, instead, make sure you push the likely scenarios you want to mitigate. You lead, not the vendor.

Then perform the tests.

Next, analyze the results. What happened? How well did the test go? Figure out strengths and weaknesses. Can you live with the weaknesses? If the product is missing something that is a key expectation and the vendor promises it is coming, get the commitment in writing with a timeline. Sales people will often promise the world, but when you ask for dates in writing, the commitments become real.

Figure out how many people hours are necessary to appropriately install, maintain and operate the

solution. Do you have the available hours to run the solution? The worst thing you can do is buy and implement a solution and it becomes shelf ware or simply neglected.

Finally, the decision. Does the solution solve a critical gap in your computer security defenses? Can you appropriately implement and support it over the long run? If the answers are yes to both, then it is a winner.

You would be surprised by how many solutions fail the realistic testing and expectations of your own environment. Once, a company I was consulting at for an entirely different project asked me to sit in on a call with a vendor of the product they were getting ready to buy. The vendor was promising the world. They could do everything. Stop all attacks, known and unknown, and so forth.

So, knowing that this customer had recently suffered their biggest breach because the attacker obtained a user's password from another compromised, unrelated website on the Internet (where the user had inappropriately re-used their corporate password) and then logged in remotely using Microsoft Remote Desktop Protocol (RDP) as the user, I asked how the vendors of the product would detect and mitigate that attack. How would the product know it was an attacker logging in remotely with the user's correct password and not an attacker with the user's correct password? And since the user had tons of access to different databases, how would the product detect the user (or attacker) siphoning data from data sources the user had valid access to? All anyone heard was crickets.

In another instance, a very popular vendor claimed that you could ask its software any question and it would immediately return that answer for every device (running the vendor's agent) in the organization. You want to know if 'xyz' process is running on how many computers? "We can answer that in seconds," said the vendor. You want to know what product is missing what Microsoft patch? "We can answer that in seconds," said the vendor. You want to know what devices are running an up-to-date antivirus program? "We can answer that in half a second," said the vendor, with a sly smile.

What the vendor did not know was that I had collected the company's IT security team ahead of time and asked them to come up with ten questions about client configurations, which if they knew the answer to, would make securing their company significantly easier. It took some prodding and initial examples, but eventually they all came up with ten really good queries.

After the vendor's demo that featured every predetermined answer coming back in seconds on their demo environment ended, we asked if we could ask ten different queries. They said, "Yes", uncomfortably. I do not think they were used to anything other than the "When can we get this product installed?" question after their awesome dog and pony show.

So, we asked our ten queries. And their product delivered none of them. They did not attempt many of them. They said they would have to install additional agents, make additional configurations or write custom queries sets. One of the few queries they did try never came back…it seemed to lock up the system and became unresponsive after that. All I know is, none of the ten best queries the IT security team wanted to know could be answered by that vendor's solution.

I think most of the potential customers the vendor presents to are so wowed by the awesome demo accomplished in the predetermined environment, they just see how "great" the product is. Of course,

it is! The vendor controlled everything. They pushed what the customer was going to see and experience.

What I recommend instead is figuring out ahead of time what you are expecting the product to do, create real-world test scenarios, and then make your new vendor go prove how well their solution works with your needs and environment and not the other way around.

Using this methodology, I have been able to pick many very good solutions. Some vendors welcome the challenge and are ready to show how your needs can be answered by their system. There are many good systems out there. They are just surrounded by a lot of junk. You just need to know the right questions to ask.

24.Conti Ransomware Declared a "National Emergency" in Costa Rica; $15 Million in Rewards Offered by US Government

by Scott Ikeda
https://www.cpomagazine.com/cyber-security/conti-ransomware-declared-a-national-emergency-in-costa-rica-15-million-in-rewards-offered-by-us-government/

The Conti ransomware that has been plaguing Windows systems around the world has ripped through the Costa Rican government since April, and has become such a persistent and damaging issue that the country has declared it a national emergency. This has prompted the US State Department to turn up the pressure on the group by offering a total of $15 million in reward money for information that leads to identification or arrest of the group's organizers.

Leaked internal information from 2021 shows that Conti operates like a legitimate tech company that employs remote working contractors, some of whom apparently are not aware that they are working for a ransomware gang. In spite of its billions of dollars in activity and churning through hundreds of these lower-level employees, core members of Conti have yet to be identified or brought to justice.

Conti ransomware group in US crosshairs after rampage through Costa Rican systems

The newly sworn-in President of Costa Rica, Rodrigo Chaves Robles, began his administration by declaring a national emergency due to the extensive damage done by a spate of Conti ransomware attacks that began on April 17.

A threat actor referring to themselves as "unc1756" has stolen at least 672 GB of data from the national government, and posted nearly all of it to the Conti ransomware dark web portal after former president Carlos Alvarado refused to pay a $10 million ransom demand just prior to the end of his

term. The same actor may have been responsible for a recent breach of Peru's national intelligence agency, which had 9.5 GB of data posted to the Conti ransomware portal shortly after the Costa Rica attacks.

There is a fierce debate over whether or not ransom demands should be paid, but as Roger Grimes (Data-Driven Defense Evangelist for KnowBe4) notes, victims are often not given much of a choice: "This is what happens in today's ubiquitous world of ransomware. If you become a victim and do not pay, they will leak your data. It is a large reason why most victims are paying today. On top of the data leak, the attackers likely have every employee's personal login credentials to any site they visited during the time the ransomware was dwelling before it went off. If Costa Rica was hosting customer-facing websites in the compromised domains, like they likely were, their customer's credentials (which are often reused on other sites and services the customers visit) are likely compromised, too. Not paying the ransom puts not only Costa Rica's own services at risk, but those of their employees and customers. It is a huge mess! … The only way to fight this is by vastly improving the security of the internet overall and educating people how to avoid the social engineering scams that most often lead to ransomware exploitation. No single point solution (e.g., firewalls, VPNs, antivirus, etc.) is going to work … Unfortunately, Costa Rica's new law, and really no one's law is doing anything to fix the overall problem (i.e., that it is very, very unlikely for cybercriminals to be caught and punished). So, what we are left with is reactive recoveries, ineffectual defenses and rewards for identification and arrests that will likely never happen."

The Conti ransomware attack campaign has impacted a number of different government agencies in Costa Rica. These include the ministries of Finance and Labor, the Costa Rican Social Security Fund and the Social Development and Family Allowances Fund. Some services run by the government treasury, such as customs and tax payment interfaces, have been disrupted since April 18. The US State Department said that the country's foreign trade has been "severely impacted" by the incident.

It is still not entirely clear exactly what was leaked through the dark web portal, but independent security researchers have analyzed a small sample of the data and found that it contains SQL databases and source code that appears to be from government websites.

The Costa Rican government's Decree No. 42542 establishes the state of national emergency, primarily granting the power to treat the Conti ransomware campaign as an enhanced form of criminal attack. But as Silas Cutler, Principal Reverse Engineer for Stairwell, points out: "While government entities like the Costa Rican Social Security Fund (CCSS) can take proactive steps (like conducting a perimeter review as a means of mitigating some of the methods Conti-affiliated access brokers use) to better secure their perimeter and react faster to issues, it will not fully prevent these types of attacks. Conti-affiliated access brokers are adept at rapidly exploiting newly-discovered vulnerabilities, gaining access to networks at speeds faster than patches can be deployed … If a group like Conti or any other sophisticated actor group is going to invest dedicated time in breaking into your network, there are a limited number of things you can do to thoroughly protect yourself. Best practices, user training and regular security testing always remain the best steps organizations can employ to defend themselves."

National emergency merits bounty from US state department

The US government is attempting to assist Costa Rica with the national emergency by incentivizing insiders to spill the beans on the core members of the Conti ransomware group, offering a total of $15 million in bounties. Up to $10 million is offered for information leading to the identification or location of the group's organizers, and an additional $5 million can be had for information that leads to the arrest or conviction of "any individual in any country" conspiring to participate in a Conti ransomware attack.

Multimillion-dollar bounties are something that the US government has increasingly turned to as for-profit cyber criminals show an increased willingness to create national emergency situations by targeting critical infrastructure. The government responded to major attacks of this nature in 2021 by issuing similar bounties on members of the REvil and DarkSide gangs. It is unclear if the bounties played any role, but both of those gangs were broken up and had servers seized after becoming the target of major international law enforcement efforts.

As John Bambenek, Principal Threat Hunter at Netenrich, notes: "The U.S. government making these rewards a bigger part of its strategy in cracking down on cybercrime and ransomware is a natural evolution of the amount of destruction these groups are causing. Ransomware in 2013 was largely an individual consumer problem. Now, these groups are hijacking entire organizations and/or leaking large caches of stolen information. They've entered the big leagues of organized crimes so now there are big league style responses. These kinds of rewards help people like me who love to research and identify these individuals. College is expensive and I have six kids. That being said, nothing is going to really help until we start making significant arrests. The initial piece of that is who to arrest, of course, however the bigger problem is that they often operate in jurisdictions where extradition isn't an option. Evgeniy Bogachev (the operator of the first modern ransomware family, Cryptolocker) has been under indictment since 2012."

The Conti ransomware group has grown to be one of the largest operators in the world by showing a willingness to cross those sorts of lines, unafraid of causing a national emergency in the process. The group has repeatedly targeted health care organizations and facilities (after declaring that it would not do so during the height of the Covid-19 pandemic), in the belief that these entities will be insured and quick to pay as they cannot afford to have life-saving systems of care be offline for any amount of time. Krebs on Security notes about 200 Conti ransomware attacks on healthcare targets in recent years, the largest of these being a breach of Ireland's national Health Service Executive public health system.

Though the key members of the group remain unidentified at this time, a leak from a dissatisfied Conti ransomware affiliate last August revealed quite a bit about the group's structure and internal operations. It has a quasi-corporate structure that includes a hiring department (that sometimes recruits on legitimate job sites), conducts performance reviews and issues "employee of the month" awards, and has a variety of online contractors working on small modular pieces of the business such that some are not aware they are involved with ransomware.

25.Diraq Emerges from Stealth; Targets Billion Qubit Silicon Quantum Computers

by Alex Challans

https://thequantuminsider.com/2022/05/10/diraq-emerges-from-stealth-targets-billion-qubit-silicon-quantum-computers/

The Sydney-based quantum computing company is the culmination of two decades of research into building quantum processors using electron spins in CMOS quantum dots and is led by Andrew Dzurak (CEO), a key figure in the field.

In March 2020, Silicon Quantum Computing announced it was ceasing its work in SiMOS. Diraq appears to be the resulting entity formed through the acquisition of IP rights.

Silicon-based qubits have been garnering more attention over the last couple of years given the potential for this technology to leverage the infrastructure and ecosystem already available in the semiconductor industry.

Whilst usable commercial systems are currently scarce (compared to superconducting and ion trap counterparts that are already accessible in the cloud) proponents argue that the approach to building quantum computers solves many of the scalability challenges.

Several other quantum computing companies are focused on silicon / spin qubits including Intel (working with QuTech), Photonic, Equal1, Silicon Quantum Computing and Quantum Motion. See our quantum market intelligence platform for a more detailed comparison of each player. Other quantum companies leveraging different qubit modalities – such as PsiQuantum in photonics – have also stressed the importance of utilizing the manufacturing footprint of working in silicon.

The company joins and increasingly rich and growing ecosystem of quantum computing companies, as covered in The Quantum Insider's Quantum Computing Market Map.

As part of its newly-launched website the business has stressed the research work and patents that underpins its technology. The business maintains 28 patents and patent applications across major jurisdictions and claims to have patents covering a detailed CMOS-based architecture for billions of qubits, capable of full error correction, advanced methods for qubit control, quantum memory, as well as innovative CMOS device designs.

Like many players in the quantum computing space, the company appears to stress that their approach is the only viable method of scaling quantum computers for wide scale commercial applications, often flagged as requiring millions, if not billions, of qubits.

The website also outlines a high-level, 3 phase roadmap:

- **Phase 1:** Accelerate development of in-house capabilities and launch fabrication of foundry services (milestone: 9-qubit logic processor, first foundry devices)
- **Phase 2:** Transition from physical to logical qubit operation and begin massive scale up of foundry services (milestone: logical qubit in silicon, 256-qubit foundry device)
- **Phase 3:** Start implementation of commercially viable algorithms and achieve a fully quantum error corrected processor (milestone: commercially viable algorithm, error-corrected processor)

The business has not yet disclosed any private VC funding but they make reference to "over $100m in funding across 9 patent families" and involvement from Allectus Capital. For more information see Diraq's website. More intel to come.

26.IBM Unveils New Roadmap to Practical Quantum Computing Era; Plans to Deliver 4,000+ Qubit System

by Hugh Collins and Erin Angelini

https://newsroom.ibm.com/2022-05-10-IBM-Unveils-New-Roadmap-to-Practical-Quantum-Computing-Era-Plans-to-Deliver-4,000-Qubit-System

IBM today (10 May 2022) announced the expansion of its roadmap for achieving large-scale, practical quantum computing. This roadmap details plans for new modular architectures and networking that will allow IBM quantum systems to have larger qubit-counts – up to hundreds of thousands of qubits. To enable them with the speed and quality necessary for practical quantum computing, IBM plans to continue building an increasingly intelligent software orchestration layer to efficiently distribute workloads and abstract away infrastructure challenges.

IBM's work to usher in an era of practical quantum computing will leverage three pillars: robust and scalable quantum hardware; cutting-edge quantum software to orchestrate and enable accessible and powerful quantum programs; and a broad global ecosystem of quantum-ready organizations and communities.

"In just two years, our team has made incredible progress on our existing quantum roadmap. Executing on our vision has given us clear visibility into the future of quantum and what it will take to get us to the practical quantum computing era," said Darío Gil, Senior Vice President, Director of Research, IBM. "With our Qiskit Runtime platform and the advances in hardware, software, and theory goals outlined in our roadmap, we intend to usher in an era of quantum-centric supercomputers that will open up large and powerful computational spaces for our developer community, partners and clients."

IBM originally announced its quantum roadmap in 2020. Since then, the company has delivered on each of the targets on its timeline. This includes IBM Eagle, a 127-qubit processor with quantum circuits that cannot be reliably simulated exactly on a classical computer, and whose architecture laid

the groundwork for processors with increasingly more qubits. Additionally, IBM has delivered a 120x speedup in the ability to simulate a molecule using Qiskit Runtime, IBM's containerized quantum computing service and programming model, compared to a prior experiment in 2017. Later this year, IBM expects to continue the previously laid out targets on its roadmap and unveil its 433-qubit processor, IBM Osprey.

In 2023, IBM will progress on its goals to build a frictionless development experience with Qiskit Runtime and workflows built right in the cloud, to bring a serverless approach into the core quantum software stack and give developers advanced simplicity and flexibility. This serverless approach will also mark a critical step in achieving the intelligent and efficient distribution of problems across quantum and classical systems. On the hardware front, IBM intends to introduce IBM Condor, the world's first universal quantum processor with over 1,000 qubits.

"Our new quantum roadmap shows how we intend to achieve the scale, quality, and speed of computing necessary to unlock the promise of quantum technology," said Jay Gambetta, VP of Quantum Computing and IBM Fellow. "By combining modular quantum processors with classical infrastructure, orchestrated by Qiskit Runtime, we are building a platform that will let users easily build quantum calculations into their workflows and so tackle the essential challenges of our time."

Introducing Modular Quantum Computing

With this new roadmap, IBM is targeting three regimes of scalability for its quantum processors.

The first involves building capabilities to classically communicate and parallelize operations across multiple processors. This will open the avenue to a broader set of techniques necessary for practical quantum systems, such as improved error mitigation techniques and intelligent workload orchestration, by combining classical compute resources with quantum processors that can extend in size.

The next step in delivering scalable architecture involves deploying short-range, chip-level couplers. These couplers will closely connect multiple chips together to effectively form a single and larger processor and will introduce fundamental modularity that is key to scaling.

The third component to reaching true scalability involves providing quantum communication links between quantum processors. To do so, IBM has proposed quantum communication links to connect clusters together into a larger quantum system.

All three of these scalability techniques will be leveraged toward IBM's 2025 goal: a **4,000+ qubit processor** built with multiple clusters of modularly scaled processors.

Building the Fabric of Quantum-Centric Supercomputing

In tandem with hardware breakthroughs, IBM's roadmap targets software milestones to improve error suppression and mitigation. Current progress being made with these techniques is improving the ability of quantum software to minimize the effect of noise on the users' application and are paving the path towards the error-corrected quantum systems of the future.

Earlier this year, IBM launched Qiskit Runtime primitives that encapsulate common quantum hardware queries used in algorithms into easy-to-use interfaces. In 2023, IBM plans to expand these primitives, with capabilities that allow developers to run them on parallelized quantum processors thereby speeding up the user's application.

These primitives will fuel IBM's target to deliver Quantum Serverless into its core software stack in 2023, to enable developers to easily tap into flexible quantum and classical resources. As part of the updated roadmap, Quantum Serverless will also lay the groundwork for core functionality within IBM's software stack to intelligently trade off and switch between elastic classical and quantum resources; forming the fabric of quantum-centric supercomputing.

The new systems targeted on IBM's expanded quantum roadmap will be designed to work within IBM Quantum System Two. Incorporating modularity and flexibility into every layer of the technology stack, IBM Quantum System Two will offer the infrastructure needed to successfully link together multiple quantum processors. A prototype of this system is targeted to be up and running in 2023.

IBM Quantum Safe

Today's announcement includes a commitment to extend IBM's security leadership to take cyber resiliency to a new level and protect data against future threats that could evolve with expected advances in quantum computing. There is significant concern that data considered securely protected today could already be lost to a future quantum adversary if stolen or harvested now for future decryption. All data – past, present, and future – that is not protected using quantum-safe security may one day be at risk. It follows that the longer that the migration to quantum-safe standards is postponed, the more data remains potentially insecure.

IBM is home to some of the best cryptographic experts globally who have developed quantum-safe schemes that will be able to deliver practical solutions to this problem. Currently, IBM is working in close cooperation with its academic and industrial partners, as well as the U.S. National Institute of Standards and Technology (NIST), to bring these schemes to the forefront of data security technologies.

Additionally, IBM is announcing its forthcoming IBM Quantum Safe portfolio of cryptographic technologies and consulting expertise designed to protect clients' most valuable data in the era of quantum.

IBM's Quantum Safe portfolio is intended to help our clients by providing:

- **Education** to understand what is different with new quantum-safe cryptography and what the implications are for an organization. Designed for security professionals and executives, IBM Quantum Safe Awareness service provides a regular flow of strategic insights for migration to the new generation of quantum-safe cryptography.

- **Strategic guidance** from IBM Consulting through the IBM Quantum Safe Scope Garage workshop. The new program will offer first-step guidance and education to prioritize quantum-safe initiatives for organizations tailored to organizational risk, IT strategy, supply-chain dependencies, and ecosystem operations.

- **Risk assessment and discovery** using automation to establish the cryptographic inventory, dependencies, and security postures. For example, the TSS zSystem Technical Services offers a zSystem Quantum Safe Assessment which allows organizations to quickly understand exposures to quantum-based cryptography attacks.

- **Migration to agile and quantum-safe cryptography** to enable organizations with modern and flexible paradigms, such as cryptographic services. For example, IBM has already implemented agile and quantum-safe cryptography to build z16, IBM's first quantum-safe mainframe system to employ quantum-safe cryptography.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

27.Recognizing Decades of Ground-Breaking Quantum Computing Research

https://www.quantinuum.com/pressrelease/recognizing-decades-of-ground-breaking-quantum-computing-research

Quantinuum today honored researchers from the National Institute of Standards and Technology (NIST) for their technical achievements and contributions to the field of quantum computing.

In a ceremony at the company's U.S. headquarters in Broomfield, President and Chief Operating Officer Tony Uttley recognized the decades of innovative research by NIST's Ion Storage Group and the role it has played in the development of Quantinuum's H-series hardware technology, which recently set an industry record for performance.

"It's impossible to overstate the impact of the NIST Ion Storage Group and its research," Uttley said. "Quantum computing has advanced to where it is today in large part because of this group and its commitment to making its work available. Their research forms the basis for the trapped ion quantum computing technologies being developed by Quantinuum and others. It is truly a technology transfer success story for the U.S. government."

NIST's Colorado-based ion trap group was formed in the late 1970s not long after Dr. David Wineland, demonstrated that by using lasers, it was possible to cool ions to low enough temperatures that they could be manipulated and controlled while trapped in electromagnetic fields.

This discovery and the team's subsequent research led to the development of some of the world's most precise atomic clocks, a technology that helps enable Global Positioning Systems (GPS) satellites.

In the 1990s, the NIST group expanded its focus to quantum information processing and quantum computing. In 1995, the NIST team successfully executed the world's first entangling two-qubit quantum gate, an operation that is key to quantum computing.

In 2000, the group demonstrated for the first time the more robust Mølmer-Sørensen gate, entangling four ion qubits. The Mølmer-Sørensen gate is at the heart of almost all ion-trap quantum computing gates today.

In 2002, the team published an article in Nature outlining the concept of the Quantum Charged Coupled Device (QCCD) architecture for a trapped ion-based quantum computer. (Quantinuum uses this QCCD architecture in its H-Series hardware, Powered by Honeywell.)

These advancements and others led to Wineland sharing the 2012 Nobel Prize for Physics with Serge Haroche for "ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems.

The NIST team continues to advance trapped ion technologies. Quantinuum recently signed an agreement with NIST to collaborate on some trap design elements.

Uttley said Quantinuum's relationship with NIST is critical to the company's success and its ongoing efforts to build the highest performing quantum computers in the world.

"The NIST team has a deep expertise in ion trap design, which will continue to help us on the technical side," Uttley said. "The agency also has trained a great number of students and researchers over the years to become leading experts in the field and helped bolster the current and future quantum workforce."

"Technology transfer is an important way that NIST achieves its mission of promoting U.S. innovation and industrial competitiveness," said Director of NIST's Physical Measurement Laboratory Jim Kushmerick. "We are always excited to see our research applied to develop commercial products, particularly those with great potential such as quantum computing."

28.Uncovering China's Deep Dive into Quantum Technology

by Liu Xun

https://news.cgtn.com/news/2022-05-07/China-sets-world-record-in-long-distance-quantum-states-transmission-19PKYksZ4eQ/index.html

Quantum computing and quantum communication are confusing concepts for most of us, and sound like futuristic technologies that have no impact on our daily lives. However, they're closer than you might think. Powerful computers, communication networks and new tools for processing information have been using quantum technologies for years.

Physicist Pan Jianwei, known as China's "father of quantum," and his team made record-setting breakthroughs in realizing quantum states transmission (QST) between two ground stations over 1,200

kilometers apart via a quantum scientific experiment satellite, signaling a giant step toward constructing a global quantum information processing and communication network.

The paper on this successful experiment, co-authored by Pan and his team, was then published in the journal Physical Review Letters on April 26.

Is quantum tech far from us?

Quantum computers could one day solve intractable problems such as identifying new chemical compounds to treat diseases, or be integrated with standard encryption techniques to create a secure network with classical relay points.

A bank account password, for example, could be securely communicated between two devices 90 kilometers away using three 30-kilometer quantum channels connected by two relay points and protected by encryption.

Yet, the most notable aspect is that the cutting-edge technology can spot any eavesdropping attempt during quantum transmission so as to safeguard information at the relay points by classical encryption.

What is QST?

Being realized by quantum teleportation, the long-distance QST is one of the key approaches for constructing quantum communication networks and essential requirement for realizing multiple quantum information processing tasks. Supported by long-distance quantum entanglement distribution, quantum states can be measured and restructured to achieve long-distance transmission which can be theoretically infinite.

As the distance and quality of quantum entanglement distribution are affected by channel loss, decoherence and other factors, how to break the transmission distance limit has always been one of scientists' biggest concerns. Using satellite-carried entanglement sources to distribute entanglement to two remote places to prepare and restructure quantum states is one of the most feasible ways to achieve so.

Nevertheless, due to the atmospheric turbulence, it is extremely difficult to measure the quantum states based on quantum interference after photons propagate in the atmospheric channel. In previous experiments, producers of QST were all quantum entanglement sources owners, it is impossible to truly use entanglement provided by a third party to realize prior distribution and follow-up transmission of quantum states.

China launches world's first quantum satellite

Over the past years, China has made several quantum technological advances including the world's first quantum satellite and optical quantum computing machine prototype, as well as a 2,000-kilometer quantum communication line between the two megacities of Beijing and Shanghai.

On August 16, 2016, China launched the world's first quantum satellite known as the Quantum Experiments at Space Scale (QUESS), nicknamed "Micius" after an ancient Chinese philosopher. Not until then, did the Chinese research team first realize entanglement and distribution between two stations over 1,000 kilometers apart with the Micius platform providing valuable entanglement distribution resources for quantum communication experiments.

In order to overcome quantum light interference following long-distance turbulent atmospheric transmission, the research team developed an optical interferometer with ultra-high stability through optical integration bonding technology which can remain stable without active loop closure for a long time and combine the quantum teleportation scheme based on two-photon path-polarization mixed entangled state.

With this technological breakthrough, the long distance QST between the Lijiang station in southwest China's Yunnan Province and the Delingha ground station in northwest China's Qinghai Province, which are 1,200 kilometers apart, was finally verified, and the transmission fidelity surpassed the classical limit with a total of six typical quantum states fully verified.

29.Wordpress Sites Getting Hacked 'Within Seconds' of TLS Certificates Being Issued

by Adam Bannister
https://portswigger.net/daily-swig/wordpress-sites-getting-hacked-within-seconds-of-tls-certificates-being-issued

Attackers are abusing the Certificate Transparency (CT) system to compromise new WordPress sites in the typically brief window of time before the content management system (CMS) has been configured and therefore secured.

CT is a web security standard for monitoring and auditing TLS (aka SSL) certificates, which are issued by certificate authorities (CAs) to validate websites' identity.

First implemented by the DigiCert CA in 2013, the standard mandates that CAs immediately record all newly issued certificates on public logs in the interests of transparency and the prompt discovery of rogue or misused certificates.

DDoS attacks

However, evidence is growing that malicious hackers are monitoring these logs in order to detect new WordPress domains and configure the CMS themselves after web admins upload the WordPress files, but before they manage to secure the website with a password.

Multiple testimonies have emerged detailing sites being hacked within minutes – within seconds, even – of TLS certificates being requested.

Domain owners report the appearance of a malicious file (/wp-includes/.query.php) and sites being press-ganged into joining DDoS attacks.

On a related thread on the support forum of Let's Encrypt, a CA that issues free certificates and launched its own CT log in 2019, a Certbot engineer said the attacks had "been happening for a few years now".

Recon techniques

Josh Aas, executive director at the Internet Security Research Group, which runs Let's Encrypt, agrees with the engineer's speculation over the attackers' reconnaissance techniques.

"If the attacker is polling CT logs directly they would see new certificate entries faster, giving them a larger time window in which to pull off the attack," Aas told The Daily Swig. Scanning crt.sh, a certificate search domain, "might also work, but it takes longer for new certificates to propagate from CT".

There's no question of the attacks reflecting shortcomings in the CT system, which according to Let's Encrypt has "led to numerous improvements to the CA ecosystem and web security" and "is rapidly becoming critical infrastructure".

Aas said all publicly trusted CAs are required to submit certificates to CT logs "without delay after they are issued".

An argument for automation

He suggested that the responsibility for protecting new WordPress sites ultimately lies with domain owners and hosting providers.

"Getting a certificate from Let's Encrypt may make it easier to detect a new installation, but nobody should be putting WordPress installations on the public internet until they are secured. If a hosting provider or any other entity is doing that, please report it as a vulnerability in their deployment process."

30.A Security Researcher Easily Found My Passwords and More: How My Digital Footprints Left Me Surprisingly Over-Ex-

posed

by Danny Palmer
https://www.zdnet.com/article/a-security-researcher-told-me-my-passwords-and-more-how-15-years-of-digital-footprints-left-me-exposed/

The internet does not like to forget.

Many of us know this, or at least it's something that's in the backs of our minds as we post updates to Facebook, share photos on Instagram, detail little insights into our daily lives on Twitter, and enter our personal data into a variety of other social media platforms and online services.

But now I can see that it's really true, for me at least.

For years, I've been writing about cybersecurity, so I'm aware of the risks around personal information being shared online and how valuable our sensitive data can be to cyber criminals – as I wrote about when someone tried to use my stolen bank details over 4,500 miles away.

It's why I'm careful with what I sign-up to, what I post, and who can see it. I make sure that my passwords are complex enough so they can't be guessed, plus whenever possible, I use multi-factor authentication to protect my accounts.

These are all habits I've developed during the past 10 years or so.

But prior to that, I was much more naive about putting personal data online, particularly when I started regularly using the internet, after getting a home computer for the first time as a teenager in around 2001.

This access opened a lot of worlds to me. I was part of gaming clans, I got my first taste of social media with MySpace, and I joined various online forums, posting comments and talking with people with similar interests – later, even meeting other users in person at group meets.

Back then, security and privacy didn't really cross my mind. Gradually, as I got older, and went to university, found and changed jobs, moved to different cities and found new hobbies, I didn't post on the forums anymore, and eventually I forgot about them.

Which is why it was startling when someone showed me how easy it was to find my username for a particular forum – and linked to a thread from the bulletin board containing almost two-decade old photos of me from a forum meetup. These old photos were innocent enough – just group photos from a London pub – but I had completely forgotten they existed, yet there they were still sitting on the open internet.

It was strange to see them and think about how they'd been sitting online for almost 20 years – and for a savvy cyber sleuth, that account could provide a pathway to finding out all sorts of other in-

formation about me and my online habits – and as I discovered, it does.

Fortunately for me, it wasn't anyone with ill-intent who'd been digging around my online history, but rather Jack Chapman, VP of threat intelligence at cybersecurity company Egress. But it gave me an insight into how this long-forgotten online profile – and other aspects of my digital footprint – were out there on the internet and how they could be abused. Because while finding old data about me had nostalgia value, in the wrong hands and against a different person, such information could be the key to unlocking a whole lot more.

"We're in the age of data and that data can easily be held by people with nefarious means," Chapman told me.

So how was it possible to track down an old forum account, along with a bunch of other information, and tie it to me?

It starts with something that, unfortunately, has happened to almost anyone who has online accounts – being involved in a data breach, where hackers have broken into online services, stolen and then leaked email addresses, passwords, contact information, credit dark details and other sensitive personal data.

It was one of these elements that was the first step to tracking down long-forgotten aspects – or so I thought – of my online footprint.

If you're using the internet, it's highly likely that you have at least one personal email address. It's what we use to sign up for various services – and there can potentially be hundreds of those, even if we only use them once before forgetting about them. And that information doesn't go away.

I have a personal email address that that's been active for almost 20 years, which has been used to sign up for many different websites and online services. Unfortunately, a number of those services have ended up being breached by cyber criminals and information about the accounts pasted online.

According to HaveIBeenPwned, that email address has been in at least 14 different breaches over the years, exposing linked information including my name, online usernames, passwords and more.

Some of these were huge data breaches that exposed the information of millions of people, such as May 2016's LinkedIn data breach that exposed 164 million email addresses and passwords, or January 2019's Collection 1 dump, a massive set of leaked and stolen data that contained 773 million usernames and passwords.

Chapman was able to use that information as a jumping-off point to search for personal data about me available online that malicious cyber criminals could potentially use against me – and it was a shock to hear him read out some of my old passwords to me.

In most cases, I knew these passwords had been revealed in breaches and previously made the effort to change each one to a unique new password. But 10 to 15 years ago when I was more naive about using the internet, I used the same password across multiple different online accounts – which meant

if one account was breached, the others were also vulnerable to being hacked.

Cyber criminals often take advantage of the way people re-use the same password. For example, someone using one password on their personal email account and the same one for their corporate account could potentially provide cyber criminals with a route into a corporate network. Alternatively, if your username and password for your email is the same as your username and password for your bank, cyber crooks will quickly discover and exploit this loophole.

Some of the breaches of my details involved some of my old online usernames related to forum accounts and online-gaming handles. By combining that information with my name and email address, it was possible to locate an old forum profile – particularly as it turned out I'd long forgotten that I'd written blogs for one of these websites, which linked my real name and user profile name together.

It was via this profile that Chapman was able to find my old forum posts, including those in the photo thread that I'd forgotten about until now – because my username was in the title for the forum thread. It was very weird seeing how someone could use leaked information to track old photos of me.

This particular bit of online history was from 2005, when I hadn't really considered online privacy as an issue. And yet over 15 years later, a determined attacker could use these – as it turned out – very public details to try to gather information about me that could be used to break into accounts or attempt to carry out phishing attacks designed around my habits.

But at least I remember posting on these forums – what was worrying was how a database of breaches, which my old email address had been involved in, included various websites I don't even remember signing up for or using.

One of these that stood out was a data breach of online game Stronghold Kingdoms in July 2018, exposing usernames, passwords and email addresses. I've heard of the game but don't remember ever signing up to play it. It's possible I did, or given the nature of games, that the studio behind it was acquired or merged with another studio, which created a previous online game I played years before. Yet my username and password were exposed in this breach.

And from there, Chapman was able to link to another data breach, at a website called Zoosk. This is another site I have no memory of at all, but it turns out to be a dating website that I apparently used in about 2010 – and that data breach gave away my date of birth and the city I was living in at the time.

Further analysis of the breach even linked it back to an IP address and an internet provider. This was a location I haven't lived in for over a decade now, but it was still unnerving to see how information on a website could be used to ultimately help trace the geolocation of where I was at the time.

All of this is sensitive information that cyber criminals could use to build a better picture of targets and to gain as much from them as possible – and, in this case, as much as possible about me.

"By having more information, it allows an attacker two key advantages – first, it allows them a better

understanding of your life and work. This allows them to tailor their attacks to improve their credibility and likelihood of success," says Chapman.

"The other opportunity is that it offers them the chance to understand your 'social network' both on a personal and work front. This is often used for robust targets, where they initially breach a more vulnerable victim in their target's close network".

In my case, that 'social network' attack would involve a cyberattacker spying on people I know or hacking their accounts to gain more information about me. If I thought an email was really sent from a friend, I might be more willing to open links contained within it. A cyber criminal who controlled that account could use that link to deliver malware or carry out other nefarious activities.

Some of the breaches my data has been exposed in are over a decade old. And the problem is that once that data is out there, it's not going away. While it's possible to change passwords, for other information – such as your name, address, online username and email address – it isn't really possible.

Our email address is often the key to our online lives. We use it to log in into social networks, banking, shopping and many other online services. Most of us stick to the email address that we've used for many years, because we're used to it, and it's tied to so many things we use everyday.

That makes it difficult to alter – imagine having to go around dozens of your online accounts and in each case going through all the steps to change your email address every time it gets leaked in a breach. But is there a case to be made for potentially discontinuing the use of an email address if it's been in too many breaches, because that could leave us vulnerable to being hacked, particularly if it's a corporate email address? Chapman thinks so.

"One thing we as an industry haven't had a conversation about is retiring email addresses. If they have been in a certain number of breaches, should we have best practice where we say, 'no, actually, that's elevating the amount of risk we're facing as a business – we should shut that down now,'" he says.

But for most of our information, once it's out there on the internet, it's out there for good and there's not much we can do about it. That means the best practice is to understand what information might be out there and to be alert about when your personal data might potentially be abused.

For example, if you know credit card details have been stolen in a data breach, it's a good idea to contact your bank, cancel that card and get a new one to avoid fraudulent activity on your account.

Meanwhile, if you get an alert from a service provider that they've been hacked and it's possible information might have been stolen, it's good practice to change your password for that account – and any other accounts that password may be used for – to stop cyber criminals abusing stolen data.

If you're aware that your details have been leaked in a breach, you should also be on the lookout for phishing emails. In many cases, leaked emails just get put on spam lists. Many of these are simple to detect – emails claiming you've won gift cards or offering free items.

But some are sneakier and will use worries around data breaches to send more targeted phishing emails. For example, when a Bitcoin trading site is the victim of a hack, other attackers look to take advantage by sending phishing emails to leaked lists of users, claiming their accounts are at risk and to 'click here' to fix it – only for that link to be a portal to steal login details and Bitcoin.

This happens with many different breaches, so it's vital that users treat emails like this with suspicion. It's unlikely that a company will inform you of a breach and include a link to log in. And if you do think there might be an issue, it's best to open your internet browser and go to the site itself, thus avoiding getting caught out by a phishing email.

If there's old accounts that you don't use anymore, it might be worth shutting them down, as they could contain a lot of personal information that could be used against you by cyber criminals. If the account doesn't exist, there's much less risk to the user.

"Unless you manually delete or change things, nothing is forgotten now – and attackers know that," says Chapman.

That's certainly the case with the old photos on the online forum. But in a frustrating twist, I checked to see if I could go back and delete the images from the forum posts, but it isn't possible – my account was automatically shut down at some point because it wasn't being used, only listing my profile as a 'former member' of the forum. But my username is in the title of the thread and the photos are still there.

There's no way to remove the photos or the connected forum posts, along with a traceable trail of information about my online history spanning almost 20 years. It's a little disturbing but serves as a reminder that personal information that ends up on the internet can end up there forever, even if it's something you'd rather forget.

31.President Biden Signs Two Executive Orders for Quantum Technology

https://quantumcomputingreport.com/president-biden-signs-two-executive-orders-for-quantum-technology/

The first Executive Order, Executive Order on Enhancing the National Quantum Initiative Advisory Committee is to enhance the National Quantum Initiative Advisory Board to place it under direct authority of the White House. Previously, members to this committee were appointed by the Secretary of Energy and now they will be appointed by the President. This board was established as a result of the National Quantum Initiative (NQI) act passed in 2018 and consists of quantum experts from industry, academia, and government with a purpose to assess trends and developments in quantum information science and technology (QIST), implementation and management of the NQI, determine whether NQI activities are helping to maintain United States leadership in QIST, recommend any program revisions that may be necessary, point out opportunities that may exist for international col-

laboration and open standards, and whether national security and economic considerations are adequately addressed by the NQI. The initial membership of the advisory board was announced in August 2020 and they have been meeting ever since.

The second Executive Order, National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, provides an outline of the U.S. government's plan to address the risks posed by quantum computers to America's cybersecurity. It directs Federal agencies to pursue a whole-of-government and whole-of-society approach to harness the economic and scientific benefits of quantum information science for all Americans, issues a directive to NIST to establish a "Migration to Post-Quantum Cryptography Project", sets requirements for Federal agencies to update cryptographic systems, and directs Federal agencies to develop comprehensive plans to safeguard American intellectual property, research and development, and other sensitive technology from acquisition by America's adversaries, and to educate industry and academia on the threats they face.

The White House has issued a fact sheet announcing these two Executive Orders that can be accessed here.

32.Hackers Stole Data Undetected from US, European Orgs since 2019

by Bill Toulas
https://www.bleepingcomputer.com/news/security/hackers-stole-data-undetected-from-us-european-orgs-since-2019/

The Chinese hacking group known as 'Winnti' has been stealthily stealing intellectual property assets like patents, copyrights, trademarks, and other corporate data – all while remaining undetected by researchers and targets since 2019.

Winnti, also tracked as APT41, is an advanced and elusive cyber-espionage group that is believed to be backed by the Chinese state and operates on behalf of its national interests.

The discovered cybercrime campaign has been underway since at least 2019 and targeted technology and manufacturing firms in East Asia, Western Europe, and North America.

Operation CuckooBees

This criminal operation is known as 'Operation CuckooBees' and was discovered by analysts at Cybereason, who revealed new malware deployed by the notorious group of hackers, the mechanisms they leverage for intrusion, and the intricate payload delivery methods they use.

> "With years to surreptitiously conduct reconnaissance and identify valuable data, it is estimated that the group managed to exfiltrate hundreds of gigabytes of information.

> The attackers targeted intellectual property developed by the victims, including sensitive documents, blueprints, diagrams, formulas, and manufacturing-related proprietary data. - Cybereason.

The financial losses incurred by "CuckooBees" are hard to determine, but the figure should be on a scale that puts the operation among the most damaging cyber campaigns of the past years.

A stealthy operation

The infection chain observed in Operation CuckooBees begins with exploiting known and zero-day vulnerabilities in ERP platforms used by the targets.

Winnti establishes persistence via an encoded WebShell, by abusing the WinRM protocol for remote access, the IKEEXT and PrintNotify Windows services for DLL side-loading, or by loading a signed kernel rootkit.

Once they gain a foothold on networks, the hackers perform reconnaissance using built-in Windows commands like 'systeminfo', 'net start',' net user', and 'dir c:\', that are unlikely to trigger any alerts for suspicious activity, even when run in batch files via a Scheduled Task.

Command	Technique
fsutil fsinfo drives	System Drives Discovery
ipconfig	System Network Configuration Discovery
nbtstat	Remote System Discovery
net accounts	Password Policy Discovery
net group	Permission Groups Discovery
net session	System Network Session Discovery
net share	Network Share Discovery
net start	System Service Discovery
net time	System Time Discovery
net use	System Network Connections Discovery
net user	Account Discovery
net view	Network Share Discovery
netstat	System Network Connections Discovery
nslookup	System DNS Configuration Discovery
ping	Remote System Discovery
query user	System Owner/User Discovery
systeminfo	System Information Discovery
tasklist	Process Discovery
tracert	Remote System Route Discovery
whoami	Logged On User Discovery

Commands used for reconnaissance (Cybereason)

For credential dumping, Winnti uses either the 'reg save' command to save the stolen passwords in a safe place or a variant of a previously undocumented tool named 'MFSDLL.exe.'

For lateral movement, the hackers continue to abuse the Windows Scheduled Tasks along with a set of special batch files.

```
SCHTASKS /Create /S <IP Address> /U <Username> /p <Password> /SC ONCE /TN test /TR <Path to a Batch File> /ST <Time> /RU SYSTEM
```

Scheduled task for lateral movement (Cybereason)

Finally, for the data collection and exfiltration, the threat actors deploy a portable command-line WinRAR app that features a valid digital signature and uses "rundll32.exe" for its executable.

WinRAR signature (Cybereason)

New findings

What stands out in Cybereason's report is a new Winnti malware dubbed "DEPLOYLOG" and the method of abuse of the Windows CLFS (Common Log File System) mechanism for payload concealing.

CLFS is an internal logging system for Windows OSes, which uses a proprietary file format that's only accessible through the system's API functions. As such, its log files are skipped by AV scanners while human inspectors don't have a tool that can parse them.

Winnti abuses this system to store and hide its payloads that are dropped on the target system in CLFS log form and then extracted and executed via CLFS API calls.

The DEPLOYLOG malware, which hasn't been documented before, is a 64-bit DLL (masqueraded as "dbghelp.dll") that extracts and executes Winnti's final payload, the WINNKIT rootkit, and then establishes two communication channels with the remote C2 and the kernel-level rootkit.

Some of the malware used to abuse Windows CLFS was previously discovered by Mandiant but had not been attributed to any threat actors.

WINNKIT is the threat actor's most evasive and sophisticated payload, which has been extensively

analyzed in the past. Still, even after all this time, it remains largely impervious to anti-virus detection.

In Operation CuckooBees, WINNKIT uses reflective loading injection to inject its malicious modules into legitimate svchost processes.

"WINNKIT contains an expired BenQ digital signature, which is leveraged to bypass the Driver Signature Enforcement (DSE) mechanism that requires drivers to be properly signed with digital signatures in order to be loaded successfully," explains the malware report by Cybereason.

"This mechanism was first introduced in Windows Vista 64-bit, and affects all versions of Windows since then."

After successful initialization, WINNKIT will hook the network communication and start receiving custom commands through DEPLOYLOG.

Defending your network

Despite indictments of Winnti members announced in the past couple of years by the U.S. Department of Justice, and no matter how many technical reports analyzing its tools and tactics have been published, the notorious Chinese cyber-espionage group remains active and industrious.

Cybereason believes that due to the complexity, stealth, and sophistication of Operation CuckooBees, it's very likely that Winnti compromised many more companies than those they were able to verify.

The best bet for defenders against such threats is to update all their software to the latest available version, monitor all network traffic, and use network segmentation.

For more details on Winnti's TTPs, check out an additional Cybereason blog piece that focuses on the techniques, or a third devoted to the malware used in the campaign.

33.When—and how—to prepare for post-quantum cryptography

by Lennart Baumgärtner, Benjamin Klein, Niko Mohr, and Anika Pflanzer
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography

While quantum computers may not be able to crack conventional encryption protocols until 2030, many cybersecurity and risk managers should evaluate their options now.

Quantum computing holds promise for problems that are out of reach for currently available high-

performance computers, potentially fueling progress in areas such as the development of life-saving pharmaceuticals or green-battery technology. However, the technology's power also poses a significant cybersecurity risk. Fully error-corrected quantum computers (which can provide highly accurate results) will be capable of overpowering commonly used traditional encryption protocols. And experts estimate that the first fully error-corrected quantum computers could be available as soon as 2030. It might seem as though cyberrisk management leaders have time to prepare, but the post-quantum cryptography (PQC) era has already begun for many companies, whether they realize it or not. For instance, increasingly connected vehicles will need to meet high security standards to protect user safety and privacy for their usable lives—which could easily extend past 2040, by which time experts believe error-corrected quantum computers will be available. While previous cyberthreats required updates to key security protocols, quantum computing will render some protocols fundamentally unsafe. Companies will need to change their protection protocols significantly, which will require time and resources to implement. However, the precise path forward is unclear because PQC solutions are still taking shape.

While most of the data that are currently in use—and stored—will not be affected, the security of vast volumes of data, critical systems, and flagship products is still at stake. Security leaders can get started by answering two significant questions: When precisely should they begin mitigation efforts, and what steps can they take to protect their organizations' data and systems? Optimal timing varies across industries as well as within organizations and dictates the options for mitigating threats from PQC. In this article, we'll share relevant considerations that can help decision makers think through these issues.

The nature of the quantum threat

When fully error-corrected quantum computers become available, the threat level for current protocols will vary. These quantum systems will be able to decrypt widely used asymmetric security protocols, such as the commonly used RSA or elliptical curve algorithms. Such protocols are mostly used to distribute secure messages (or keys) through public networks such as the public internet. With these protocols, anyone can encrypt a message, but only the original sender has the key for decrypting it. However, quantum computing will make it possible to decode an encrypted message without this key, rendering encrypted messages legible[3].

On the other hand, symmetric encryption protocols, in which the sender and receiver exchange encryption and decryption keys before trading information, are currently assumed to be safe from quantum threats. Unfortunately, it isn't always practical to use these protocols for the speedy exchange of information through public networks, because they rely on correspondents securely trading cryptography keys before exchanging data. Managing the substantial number of keys necessary when exchanging large amounts of messages also comes with considerable computing costs. Consequently, efficiently sharing such symmetric keys is a critical issue that needs to be addressed before using these protocols.

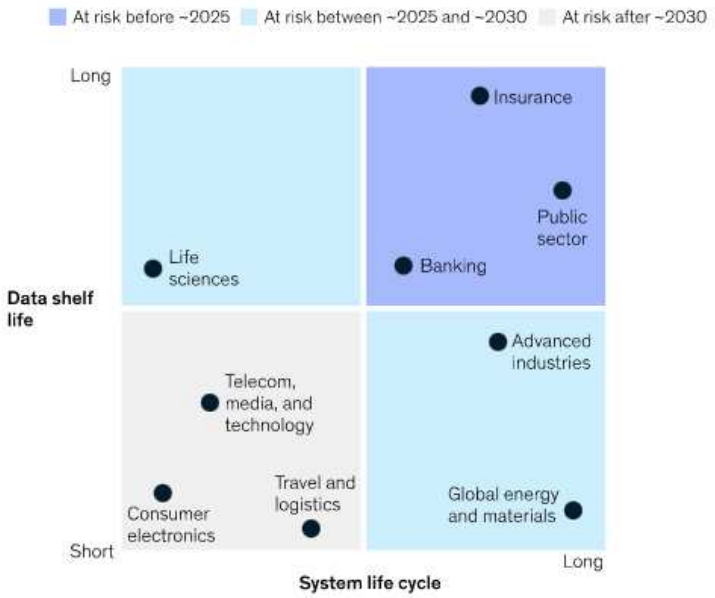
[3] While quantum computers will be able to break some asymmetric cryptography algorithms by means of Shor's algorithm, this does not imply that all asymmetric protocols can be broken (for more, see sidebar, "Overview of post-quantum cryptography solutions").

When to act: Two factors to assess

Understanding the value of cybersecurity for an organization is typically the first step in traditional security assessments, both in general and for the protection of specific systems and products. Measuring the value exposed to these risks is key to formulating appropriate strategies against threats and responses to potential security breaches. Since fully error-corrected quantum computers are not available yet, quantum security strategies start with the question of timing. Risk managers will need to examine two key characteristics of high-priority assets—data shelf life and system life and development cycles—in detail to determine when to begin quantum mitigation measures.

Industries should prepare for post-quantum cryptography based on data shelf life and system lifetime.

Risk of quantum-powered attack by industry



These two factors should be considered together. Broadly speaking, organizations with substantial value at risk that have data with long shelf lives and systems or products with extended life or development cycles should formulate their responses to PQC now. Those possessing either data or systems with longer lives may have a bit more time to act. Organizations with data and systems of shorter duration have longer still.

Consider data shelf life. Some data produced today—such as classified government data, personal health information, or trade secrets—will still be valuable when the first error-corrected quantum computers are expected to become available. For instance, a long-term life insurance contract may already be sensitive to future quantum threats because it could still be active when quantum computers become commercially available. Any long-term data transferred now on public channels will be at risk of interception and future decryption.

Because regulations on PQC do not yet exist, the possibility of data transferred today being decrypted in the future does not yet pose a compliance risk. For the moment, far more significant are the future

consequences for organizations, for their customers and suppliers, and for those relationships. However, regulatory considerations will also become relevant as the field develops, which could speed up the need for some organizations to act[4].

Just as with data, some critical physical systems developed today—the hardware and, to a lesser extent, software used to collect, process, and store data and a company's products—will still be in use when the first fully error-corrected quantum computer is expected to come online. This applies particularly to systems and products with long development timelines and operational lifetimes of more than ten years, as well as products with long manufacturing schedules.

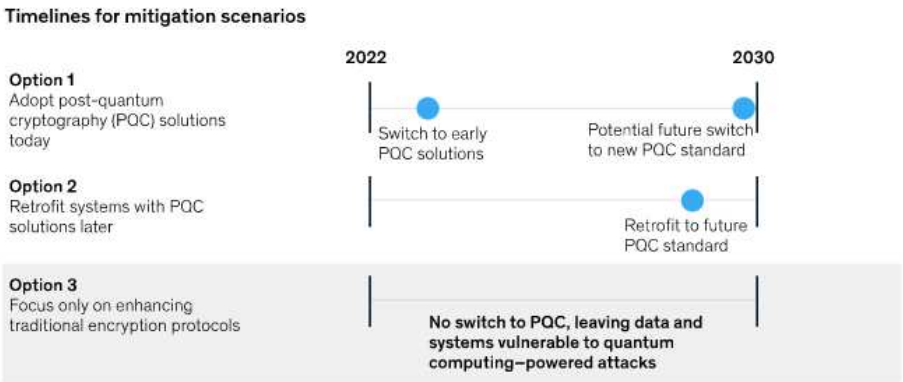
For example, automotive manufacturers are developing highly connected vehicles that must meet high security standards to protect users' safety and privacy. With development cycles of approximately five years, production cycles of about seven years, and vehicle lifetimes of roughly ten years, a car developed today will likely still be on the road after 2040. As a result, over-the-air updates for these vehicles will be particularly sensitive to quantum threats. Many government systems have long lifetimes as well, often because they can be difficult to update due to the associated costs and regulations.

Before deciding on a mitigation pathway, data, system, and product owners should create a shared internal understanding of how sensitive their various data types and systems are to quantum threats based on these two factors. Ideally, this would be done as part of standardized data cataloging and risk assessment.

Mitigating quantum threats

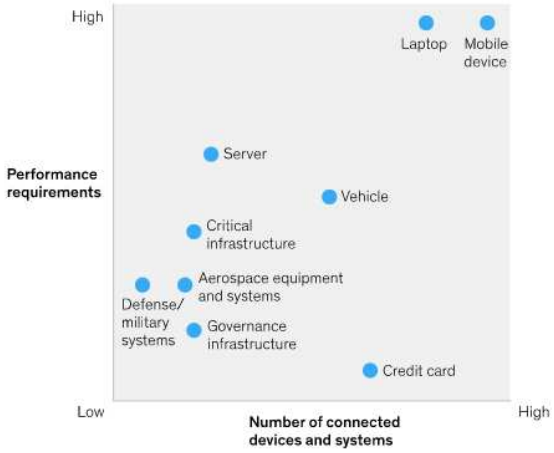
At a high level, decision makers can pursue one of three paths to mitigate the threats posed by capable quantum systems: adopt PQC solutions today, retrofit existing systems to PQC standards at a later date, or take action only to enhance the efficacy of traditional encryption protocols—all while monitoring evolving industry standards and regulations. The precise decisions will depend largely on when organizations need to begin mitigation, on the performance requirements of cryptography protocols, and on the number and distribution of connected devices and systems that require protection.

Decision makers have three options for mitigating post-quantum cryptography threats.



[4] The US National Institute of Standards and Technology (NIST) is currently evaluating different post-quantum public-key cryptographic algorithms, with the final results expected to be published in 2022.

Decisions about adopting post-quantum cryptography should account for performance requirements and the number of devices and systems that need protection.



Option 1: Adopt post-quantum cryptography solutions today

Many start-ups and a few established cryptography players already offer provisional commercial PQC solutions. While adopting one of these solutions might seem to be the best path for any company that needs to act today, there are trade-offs and drawbacks to consider (for more on these PQC solutions, see sidebar, "Overview of post-quantum cryptography solutions").

The first consideration is cost. PQC solutions currently make up only about 2 percent of the global cryptography market[5]. Without the benefits of deep penetration and scale, PQC solutions cost more than traditional cryptography solutions. Organizations that need to secure large amounts of data, devices, and systems in their networks and protocols will experience this limitation most acutely.

Second, because PQC solutions are still nascent and because it is impossible to test them against quantum computers that do not yet exist, they haven't been conclusively proven to provide protection from quantum—or even conventional—threats. As a result, organizations will need to acquire both conventional and PQC solutions to ensure the highest possible level of security if they take action today. Organizations also risk having to switch to higher-performance PQC solutions that come to market in the future, particularly if a currently available solution is excluded from future regulations. Consider that some protective algorithms have already been eliminated by a major US agency, with a few candidates remaining in the final round of reviews[6].

Third, currently available PQC solutions require significant additional computing power and higher la-

[5] Based on the Quantum Insider's 2022 Quantum security market report; "The Quantum Insider report forecasts quantum security market worth $10 billion by 2030," Quantum Insider, February 2, 2022.

[6] For more information, see "Post-quantum cryptography (PQC): Post-quantum cryptography standardization," NIST, March 10, 2022.

tency times compared with existing standards. While both measures are expected to improve, today's solutions are impractical for organizations that require low-latency performance over public channels. This includes any organization that runs high-value edge- and cloud-computing applications that require large volumes of data to flow quickly between local nodes and decentralized sources of computing power. However, today's PQC solutions may be sufficient for applications with lower latency requirements, such as nonurgent, simple bank transfers or the transfer of insurance contracts.

Given the risks and costs outlined here, most organizations should take a wait-and-see approach to PQC solutions. The exceptions are organizations and uses for which the stakes for security are particularly high, such as in the defense industry, where even provisional PQC protection for some high-value systems or for data with long lifetimes outweighs trade-offs in cost or performance. Another exceptional circumstance is when it would be more costly or impractical—or impossible—to access and retrofit high-value systems in the future compared with installing some protection today.

Option 2: Retrofit systems with post-quantum cryptography solutions later

Companies that choose to wait to adopt PQC for financial, technical, or other reasons still have some work to do today.

First, they should ensure that their hardware and software architectures can be retrofitted as easily as possible. Measures such as reserving computational resources for future cryptography updates or making the architecture sufficiently modular can simplify adding and exchanging cryptography modules in the future. In line with traditional security measures, hardware and software should be separate so that systems can remain flexible to emerging PQC algorithms.

Second, organizations should prepare, both operationally and financially, for retrofitting. Systems will need to be accessible and updated with PQC solutions, possibly while in use or while highly distributed. Some of these changes can be made remotely with software updates, but PQC solutions with high performance requirements will likely rely on specialized hardware, meaning that affected devices will need to be accessed physically in order to retrofit them. Companies responsible for a large number of devices or systems, such as consumer-electronics or auto manufacturers, risk facing operational complexities and high costs when choosing this option, so it's important to begin planning accordingly today.

Finally, organizations should begin building long-term relationships with relevant suppliers, regulators, and peers within and outside of their industries as soon as possible. These relationships will be critical for staying up to date on emerging standards and solutions for PQC. In particular, recent supply chain challenges for hardware components have illustrated the importance of relationships with suppliers. Investing in relationships with suppliers that are already working on PQC-specific hardware can provide a significant advantage when the time comes to procure equipment to retrofit systems. Plus, collaborating with peers is likely to create more benefits than hoarding expertise and capabilities; collectively developing solutions, for example, could cost less than if an organization devised solutions on its own.

Option 3: Focus only on enhancing traditional encryption protocols

Organizations with the most time to act and little value at risk to quantum threats may choose not to make the switch to PQC for the foreseeable future.

Nevertheless, these organizations should consider traditional mitigation actions, particularly extending asymmetric key lengths and using symmetric cryptography where possible. Longer keys would keep companies ahead of early versions of error-corrected quantum computers because those keys require many more qubits (or "quantum bits," the basic building blocks of quantum computers) to break. Concretely, moving from RSA-1024 to RSA-2048 encryption may extend security lifetimes by one to three years.

For more protection, organizations should consider scaling up other security measures, such as symmetric key lengths, for particularly sensitive data. Decision makers should also begin planning for future updates to long-lasting systems by, for instance, evaluating the modularity of their technological architecture.

To be sure, forgoing PQC-specific measures creates some risk for companies and their customers. After all, without PQC investments, any application requiring asymmetric encryption will be vulnerable to a fully error-corrected quantum system sooner or later. However, as with any risk, organizations must weigh the costs of increasing protection against the costs of a breach.

34.Building A Better Quantum Bit: New Qubit Breakthrough Could Transform Quantum Computing

by Bill Wellock
https://phys.org/news/2022-05-quantum-bit-qubit-breakthrough.html

You are no doubt viewing this article on a digital device whose basic unit of information is the bit, either 0 or 1. Scientists worldwide are racing to develop a new kind of computer based on the use of quantum bits, or qubits, which can simultaneously be 0 and 1 and could one day solve complex problems beyond any classical supercomputers.

A team led by researchers at the U.S. Department of Energy's (DOE) Argonne National Laboratory, in close collaboration with FAMU-FSU College of Engineering Associate Professor of Mechanical Engineering Wei Guo, has announced the creation of a new qubit platform that shows great promise to be developed into future quantum computers. Their work is published in Nature.

"Quantum computers could be a revolutionary tool for performing calculations that are practically impossible for classical computers, but there is still work to do to make them reality," said Guo, a paper

co-author. "With this research, we think we have a breakthrough that goes a long way toward making qubits that help realize this technology's potential."

The team created its qubit by freezing neon gas into a solid at very low temperatures, spraying electrons from a light bulb onto the solid and trapping a single electron there.

While there are many choices of qubit types, the team chose the simplest one—a single electron. Heating up a simple light filament such as you might find in a child's toy can easily shoot out a boundless supply of electrons.

One important quality for qubits is their ability to remain in a simultaneous 0 or 1 state for a long time, known as its "coherence time." That time is limited, and the limit is determined by the way qubits interact with their environment. Defects in the qubit system can significantly reduce the coherence time.

For that reason, the team chose to trap an electron on an ultrapure solid neon surface in a vacuum. Neon is one of only six inert elements, meaning it does not react with other elements.

"Because of this inertness, solid neon can serve as the cleanest possible solid in a vacuum to host and protect any qubits from being disrupted," said Dafei Jin, an Argonne scientist and the principal investigator of the project.

By using a chip-scale superconducting resonator—like a miniature microwave oven—the team was able to manipulate the trapped electrons, allowing them to read and store information from the qubit, thus making it useful for use in future quantum computers.

Previous research used liquid helium as the medium for holding electrons. That material was easy to make free of defects, but vibrations of the liquid-free surface could easily disturb the electron state and hence compromise the performance of the qubit.

Solid neon offers a material with few defects that doesn't vibrate like liquid helium. After building their platform, the team performed real-time qubit operations using microwave photons on a trapped electron and characterized its quantum properties. These tests demonstrated that solid neon provided a robust environment for the electron with very low electric noise to disturb it. Most importantly, the qubit attained coherence times in the quantum state competitive with other state-of-the-art qubits.

The simplicity of the qubit platform should also lend itself to simple, low-cost manufacturing, Jin said.

The promise of quantum computing lies in the ability of this next-generation technology to calculate certain problems much faster than classical computers. Researchers aim to combine long coherence times with the ability of multiple qubits to link together—known as entanglement. Quantum computers thereby could find the answers to problems that would take a classical computer many years to resolve.

Consider a problem where researchers want to find the lowest energy configuration of a protein made of many amino acids. These amino acids can fold in trillions of ways that no classical computer has

the memory to handle. With quantum computing, one can use entangled qubits to create a superposition of all folding configurations—providing the ability to check all possible answers at the same time and solve the problem more efficiently.

"Researchers would just need to do one calculation, instead of trying trillions of possible configurations," Guo said.

35.Hackers Used The Log4J Flaw to Gain Access Before Moving Across A Company's Network, Say Security Researchers

by Danny Palmer
https://www.zdnet.com/article/heres-how-hackers-used-the-log4j-flaw-to-gain-access-before-moving-across-a-companys-network/

A North Korean hacking and cyber-espionage operation breached the network of an engineering firm linked to military and energy organisations by exploiting a cybersecurity vulnerability in Log4j.

First detailed in December, the vulnerability (CVE-2021-44228) allows attackers to remotely execute code and gain access to systems that use Log4j, a widely used Java logging library.

The ubiquitous nature of Log4j meant cybersecurity agencies urged organisations globally to apply security updates as quickly as possible, but months on from disclosure, many are still vulnerable to the flaw.

According to cybersecurity researchers at Symantec, one of those companies that was still vulnerable was an undisclosed engineering firm that works in the energy and military sectors. That vulnerability resulted in the company being breached when attackers exploited the gap on a public-facing VMware View server in February this year. From there, attackers were able to move around the network and compromise at least 18 computers.

Analysis by Symantec researchers suggests that the campaign is by a group they call Stonefly, also known as DarkSeoul, BlackMine, Operation Troy, and Silent Chollima, which is an espionage group working out of North Korea.

Other cybersecurity researchers have suggested that Stonefly has links with Lazarus Group, North Korea's most infamous hacking operation.

But while Lazarus Group's activity often focuses on stealing money and cryptocurrency, Stonefly is a specialist espionage operation that researchers say engages in highly selective attacks "against targets that could yield intelligence to assist strategically important sectors" – including energy, aero-

space, and military.

"The group's capabilities and its narrow focus on acquiring sensitive information make it one of the most potent North Korean cyber-threat actors operating today," warn researchers at Symantec.

Stonefly has existed in some capacity since 2009, but in recent years it has doubled down on targeting highly sensitive information and intellectual property. This is achieved by deploying password-stealers and trojan malware on compromised networks. In the case of the undisclosed engineering firm, the first malware had been dropped onto the network within hours of the initial compromise.

Among the tools deployed in this incident was an updated version of Stonefly's custom Preft backdoor malware. The payload is delivered in stages. When fully executed, it becomes an HTTP remote access tool (RAT) capable of downloading and uploading files and information, along with the ability to download additional payloads, as well as uninstalling itself when the malware is no longer needed.

Alongside the Preft backdoor, Stonefly also deployed a custom-developed information-stealer that the attackers planned to use an alternative means of exfiltration.

Stonefly has been active for over a decade and it's unlikely their attacks will stop soon, particularly as the group has a history of developing new tactics and techniques. While Stonefly is classified as a powerful state-backed hacking group, in this instance, they didn't need advanced techniques to breach a network, they simply took advantage of an unpatched critical security vulnerability.

To help make sure known vulnerabilities like Log4j can't be exploited by state-backed hacking groups or cyber criminals, organisations should ensure that security updates for applications and software are rolled out as soon as possible. In the case of the firm above, this process would have involved applying the available patches for VMware servers, which were available before the attack happened.

Other cybersecurity protocols, such as providing users with multi-factor authentication, can also help prevent attacks that take advantage of stolen passwords to move around networks.

36.Quantum Mechanics-Based Random Number Generator to Enable Blockchain Gambling

by Michael Bodley

https://blockworks.co/quantum-mechanics-based-random-number-generator-to-enable-blockchain-gambling/

A random number generator that relies on quantum mechanics to produce smart contract-driven data sets empowered by blockchain technology has launched on more than a dozen cryptocurrency proto-

cols.

API3, in partnership with a group of researchers from the Australian National University's Quantum Optics Group, has dubbed its new product, ANU QRNG, the first "true" random number generator for smart contracts.

Ten of the 13 blockchains the startup is launching on don't yet have a random number generator available, the company told Blockworks. Some of those protocols use a random number generator that doesn't employ quantum technology — meaning their data set is limited, or a "pseudo random number," in industry speak.

A truly randomized dataset, combined with blockchain technology, allows for a number grouping for the likes of crypto gambling that cannot be manipulated to serve the needs of the house. To produce random numbers now, the company said, startups use what amounts to a "random" seed phrase that allows for the data set to be predicted — and perhaps taken advantage of — if the holder or a nefarious third party wants to do so.

"Say we take something simple, like a coin flip, for example," Ugur Mersinlioglu, product manager at API3, said. "If you have a conflict with a 'pseudo' random number, you're going to notice, at some point, that certain patterns are going to be repetitive...Whereas, if you have a process that practically doesn't spit out any detectable patterns, you can actually say that this is not capable of [manipulation] by anybody."

The quantum randomness in this case stems from measuring the random fluctuations in phase and amplitude of an electromagnetic field in a vacuum, according to the project documentation.

The service is available on blockchains including Avalanche, Fantom, Metis, Moonbeam, Polygon and RSK — with plans for additional future integrations.

The company doesn't make money on the random number generation, instead tapping it as a loss-leader into its other product lines, such as its oracle solutions and data integration services, including a validation pool that relies on staking its native token to function.

$37.2 \times N$ Twin-Field Quantum Key Distribution Network Configuration

by Karine
https://thequantumhubs.com/2xn-twin-field-quantum-key-distribution-network-configuration/

Developing Quantum Key Distribution (QKD) has been recently directed toward distance extension and network expansion for real-world secure communications. Considering a recent report on a quantum communication network over 4,600 km, it seems that QKD networks using conventional protocols have

been sufficiently studied.

However, although the twin-field QKD (TF-QKD) proposed for long-distance QKD has been studied deeply enough to succeed the demonstrations over 428- and 511-km deployed fibers, TF-QKD networks have been verified only for a ring network.

In this work, scientists propose a star topological $2 \times$ NTF-QKD network scheme, where the coherence maintenance issue, being the primary obstacle to implementing TF-QKD, can be minimized by the automatic mode-matching feature of the Sagnac-based plug-and-play architecture. A lower number of active controllers is required for this scheme in comparison with one-way TF-QKD networks.

Moreover, this scheme adopts a cost-effective configuration that requires only a single pair of single-photon detectors for the entire network system.

The team conducted a proof-of-concept experiment over a 50-km fiber successfully, achieving an average secret key rate of 1.31×10^{-4} bit per pulse (1.52 bit per second) with the finite-size effect.

38.Quantum Future: Developing The Next Generation of Quantum Algorithms and Materials

by Sarah Wong
https://scitechdaily.com/quantum-future-developing-the-next-generation-of-quantum-algorithms-and-materials/

Simulating a Quantum Future

Quantum computers are anticipated to revolutionize the way researchers address complex computing problems. These computers are being developed to address major challenges in fundamental scientific fields such as quantum chemistry. In its present state of development, quantum computing is very susceptible to noise and disruptive influences in the environment. This makes quantum computers "noisy," since quantum bits, or qubits, lose information when they go out of sync, a process known as decoherence.

To address the constraints of current quantum computers, researchers at Pacific Northwest National Laboratory (PNNL) are constructing simulations that demonstrate how quantum computers work.

"When we try to directly observe the behavior of quantum systems, like qubits, their quantum states will collapse," explained PNNL Computer Scientist Ang Li. Li is also a researcher at the Quantum Science Center and the Co-Design Center for Quantum Advantage, two of the five Department of Energy National Quantum Information Science Research Centers. "To get around this, we use simulations to

study qubits and their interaction with the environment."

Li and collaborators at Oak Ridge National Laboratory and Microsoft employ high-speed computing to create simulators that imitate genuine quantum devices for executing sophisticated quantum circuits. They recently integrated two distinct kinds of simulations to produce the Northwest Quantum Simulator (NWQ-Sim), which is used to test quantum algorithms.

"Testing quantum algorithms on quantum devices is slow and costly. Also, some algorithms are too advanced for current quantum devices," said Li. "Our quantum simulators can help us look beyond the limitations of existing devices and test algorithms for more sophisticated systems."

Algorithms for quantum computers

Nathan Wiebe, a PNNL joint appointee from the University of Toronto and an affiliate professor at the University of Washington, is taking a different approach to writing quantum computer code. Though being constrained by the capabilities of existing quantum devices might be irritating at times, Wiebe views this obstacle as an opportunity.

"Noisy quantum circuits produce errors in calculations," said Wiebe. "The more qubits that are needed for a calculation, the more error-prone it is."

Wiebe and collaborators from the University of Washington developed novel algorithms to correct for these errors in certain types of simulations.

"This work provides a cheaper and faster way to perform quantum error correction. It potentially brings us closer to demonstrating a computationally useful example of a quantum simulation for quantum field theory on near-term quantum hardware," said Wiebe.

Dark matter meets quantum computing

While Wiebe seeks to reduce the noise by developing error-correcting algorithms, physicist Ben Loer and his colleagues turn to the environment to manage external sources of noise. Loer employs his experience in creating ultra-low levels of natural radioactivity, which is required to search for experimental evidence of dark matter in the universe, to aid in the prevention of qubit decoherence.

"Radiation from the environment, such as gamma rays and X-rays, exists everywhere," said Loer. "Since qubits are so sensitive, we had an idea that this radiation may be interfering with their quantum states."

To test this, Loer, project lead Brent VanDevender, and colleague John Orrell, teamed up with researchers at the Massachusetts Institute of Technology (MIT) and MIT's Lincoln Laboratory **used a lead shield to protect qubits from radiation**. They designed the shield for use within a dilution refrigerator—a technology used to produce the just-above-absolute-zero temperature necessary for operating superconducting qubits. They saw that qubit decoherence decreased when the qubits were protected.

While this is the first step toward understanding how radiation affects quantum computing, Loer plans to look at how radiation disturbs circuits and substrates within a quantum system. "We can simulate and model these quantum interactions to help improve the design of quantum devices," said Loer.

Loer is taking his lead-shielded dilution refrigerator research underground in PNNL's Shallow Underground Laboratory with the help of PNNL Chemist Marvin Warner

"If we develop a quantum device that doesn't perform as it should, we need to be able to pinpoint the problem," said Warner. "By shielding qubits from external radiation, we can start to characterize other potential sources of noise in the device."

Creating a quantum ecosystem in the Pacific Northwest

PNNL supports a wide variety of quantum-related research, from quantum simulations and developing algorithms for quantum chemistry to the development of precision materials for quantum devices.

PNNL also partners with other institutions in the Pacific Northwest to accelerate quantum research and develop a quantum information science-trained workforce through the Northwest Quantum Nexus (NQN). Additionally, the NQN hosts a seminar series featuring leaders in quantum research. The NQN synergizes partnerships between companies, such as Microsoft and IonQ, as well as the University of Oregon, the University of Washington, and Washington State University.

"PNNL's cultivation of both industry and university collaborations are building a foundation for quantum computing in the Pacific Northwest that sets the stage for future hybrid classical-quantum computing," said James (Jim) Ang. Ang is the chief scientist for computing and PNNL's sector lead for the Department of Energy (DOE) Advanced Scientific Computing Research program.

Li's research was supported by the DOE Office of Science (SC), National Quantum Information Science Research Centers: Quantum Science Center and Co-Design Center for Quantum Advantage. He was also supported by the Quantum Science, Advanced Accelerator laboratory-directed research and development initiative at PNNL.

Wiebe's research was supported by the DOE, SC, Office of Nuclear Physics, Incubator for Quantum Simulation, and the DOE QuantISED program. Wiebe is also supported by DOE, SC, National Quantum Information Science Research Centers, Co-Design Center for Quantum Advantage, where he is the Software thrust leader.

Loer's research was supported by the DOE, SC, Office of Nuclear Physics and Office of High Energy Physics. Warner's research was supported by the DOE, SC, National Quantum Information Science Research Centers, Co-Design Center for Quantum Advantage.

39.Seismic Sensing Using Quantum Cryptography Network

by Michael Schirber
https://physics.aps.org/articles/v15/63

One form of quantum cryptography involves an optical fiber network over which users share encryption keys—strings of bits used to encode and decode messages. Fiber networks can also be used to sense earthquakes, and now researchers have shown that the two tasks could be combined[7]. The team sent a quantum key distribution (QKD) signal over a 658-km-long fiber while causing the fiber to vibrate at a specific location. They detected this vibration via the optical signal and showed that they could determine its position to within 1 km. The new technique could potentially piggyback on QKD networks currently being set up in China, South Korea, and other countries.

QKD researchers are developing techniques for sending keys over optical fibers and through wireless technologies. A common fiber protocol, called twin-field quantum key distribution (TF-QKD), obtains secure, long-distance encryption using photon interference. Detecting that interference requires constant monitoring of the light signals that users share across each fiber link. Jiu-Peng Chen from the University of Science and Technology of China and his colleagues realized that they could use this continuous data stream to detect vibrations along the fiber. "We demonstrated the possibility to collect vibration sensing data without adding new fiber or hardware resources to a TF-QKD network," says team member Qiang Zhang.

A TF-QKD experiment consists of two optical setups—called Alice and Bob—at opposite ends of an optical fiber. Each setup generates a random string of bits and sends it as an optical signal over the fiber to an intermediate node called Charlie. At Charlie, the two signals interfere, and the resulting optical signals are then transmitted back to Alice and Bob, who use the interference outcomes to generate a shared key.

Zhang and colleagues demonstrated TF-QKD in a lab setting with optical fiber wrapped around spools. The total fiber length of 658 km was one of the longest fiber-based QKD demonstrations to date (a recent experiment reached 834 km[8]). Using this fiber link, the team explored the vibrational signatures hidden in their data. As is common for the TF-QKD method, Zhang and colleagues designed their system to correct for fluctuations in the phase of light passing through the fiber. For example, if a sudden movement briefly extends the length of Alice's fiber by a half wavelength (equal to a phase fluctuation of π radians), a trough of the light wave would arrive at Charlie instead of a peak. So a TF-QKD system must continuously make adjustments—such as stretching the length of fiber by incremental amounts—to cancel out phase fluctuations. "We have spent a major effort to compensate the phase fluctuation in the channel while building our TF-QKD system," Zhang says.

---

[7] J.-P. Chen, "Quantum key distribution over 658 km fiber with distributed vibration sensing," Phys. Rev. Lett. 128, 180502 (2022).

[8] S. Wang et al., "Twin-field quantum key distribution over 830-km fibre," Nat. Photon. 16, 154 (2022).

The team showed that this fluctuation-compensation system can be used to detect a seismic vibration by installing a piezoelectric device that wiggled Alice's fiber at a specific location. The vibration frequency was set between 1 and 1000 Hz, which is the relevant range for seismic sensing. The vibrations produced phase changes between 0.9 and 50 radians, which the fluctuation-compensation system picked up. Zhang says that seismic waves should produce much larger phase changes, in the range of several hundred to several thousand radians[9]. The team performed a similar test on the frequency calibration link—a separate fiber that is required by TF-QKD systems to lock the frequencies of Alice's and Bob's lasers together. The researchers used this link to pinpoint the location of the vibration source with a precision of 1 km.

"Detecting vibration at such a long distance is impressive," says quantum information expert Hoi-Kwong Lo from the University of Toronto. He notes that similar techniques have been developed to sense vibrations along optical fibers, such as a recent experiment that used underwater telecommunication fibers to detect earthquakes. One of the authors of that paper, Giuseppe Marra from the National Physical Laboratory in the UK, says that the new QKD demonstration follows the same concept as his and other previous work. "Future QKD links based on this technique could provide useful additional seismic information from installed fibers," he says.

40.Is Fully Homomorphic Encryption Now A Reality?

by Nigel Smart
https://cybersecurity-magazine.com/is-fully-homomorphic-encryption-now-a-reality/

We all know the problems with users picking weak passwords, whether it is "PassW0rd123" or "JamesBond007". We also know that there are lists of passwords which have been obtained from hacks into websites, and from these we can work out what are the most commonly used weak passwords in circulation. Surely there must be a way of checking, when a user chooses a new password for a website, whether the password lies on the known list of common weak passwords? There are two obvious solutions to this problem: Firstly, the browser could maintain the list of weak passwords locally on the user's computer. This solution however does not scale as the list is huge, and needs to be continually updated. The second solution is for the new password to be sent to a central site and compared against the list of common weak passwords. But this solution then leaks the new (potentially strong) password to the central site doing the checking. Is there a better way?

The answer is yes, and it comes from what at first sight seems an unlikely technology. The problem one is trying to solve with password checking is known "Private Set Intersection" (or PSI) in the cryptographic literature. We have two parties with two sets; the user with a set consisting of one element, namely their password; and the central site with a huge set of common weak passwords. The goal is to determine if the two sets intersect, without revealing anything about the set sets. Such a problem

[9] G. Marra et al., "Ultrastable laser interferometry for earthquake detection with terrestrial and submarine cables," Science 361, 486 (2018).

can now be solved very efficiently using a form of cryptography called Homomorphic Encryption (HE). For many years Homomorphic Encryption has been considered highly inefficient and not usable in real-life scenarios, yet this has now changed. Indeed a HE based solution to the PSI problem is now embedded into Microsoft's Edge browser. So how come this unusable technology, is now usable?

To understand this change we have to look at the past, and introduce some terminology. A Homomorphic Encryption scheme allows a party to encrypt data (for example entries in a database, a vote in an election, or whatever) and then a second party can perform computations on the resulting ciphertexts. These computations produce a new ciphertext which encrypts a result. The result being what would have happened if they had computed on the underlying messages and then encrypted the result. Thus HE allows one to "compute on encrypted data".

There are, essentially, three types of HE schemes in deployment or development today. **The first is "linear" homomorphic encryption**. This variant allows one to compute linear functions (basically additions) on the ciphertexts. Thus a linear HE scheme can be used in a voting application, where one wants to sum up how many people voted for a given candidate, or it can be used to compute the average of an encrypted column in a database. **The second type is "Somewhat" Homomorphic Encryption (or SHE)**, this allows one to compute more complex functions on the encrypted data, and not just linear functions. For example it could be used to compute an encrypted standard deviation. **The third type is "Fully" Homomorphic Encryption (or FHE)**, this allows one to compute arbitrary complex functions on the encrypted data.

FHE had been postulated in the mid 1970's, and linearly Homomorphic Encryption schemes had been known since the 1990s. Indeed many online electronic voting systems (for example a popular one called Helios) have used such linear HE schemes for around fifteen years. More complex HE schemes were not known until a breakthrough result in 2009 by Craig Gentry (then a PhD student at Stanford University). Gentry invented an SHE scheme, and then showed a method to turn his SHE scheme into an FHE scheme; using a method he dubbed "bootstrapping". Gentry's result created a huge interest in the field, with major investments being made into research into this technology by governments, industry and academia. IBM and Microsoft formed groups working on this technology, and the US Government invested in the technology via the DARPA funded PROCEED programme.

The original schemes in 2009 were very slow, and would take many minutes to simply compute the AND of two bits. But, as time progressed, our understanding of the mathematics has improved, the schemes have become more efficient and more expressive, and implementations have been improved. The PSI scheme mentioned above from Edge is implemented using a SHE scheme, whereas FHE schemes can now be used to evaluate (some) neural networks on encrypted data.

The number of companies working on HE technology has grown considerably. IBM and Microsoft, have been joined by Alibaba, Google, Intel, Meta, Samsung, SAP, … the list goes on. There are a number of startup's working on technology in this space; most notably Duality and Enveil in the United States, and Inpher and Zama in Europe. Standards bodies are looking into standardizing the technology; there is an effort being run in one of the working groups of the International Standards Organization (ISO).

So what does the future look like for HE? The current technologies for HE are orders of magnitude

faster than the first generation schemes from 2009, but are still a little too slow for many applications. However, this performance cost is likely to reduce significantly in the coming few years. A number of companies are developing hardware acceleration engines for HE computations, a bit like graphics cards were created to accelerate graphics calculations. These accelerators are built using novel computing architectures, for example one proposal aims to use optical computing to accelerate HE computations. The US government has again made a big bet in this space, via the DARPA funded DPRIVE programme; which aims to develop hardware accelerators for HE. The DARPA programme, is matched by other companies across the world also investing in hardware HE accelerators. Once these accelerators come online one can expect (at least) a couple of orders of magnitude performance improvement in HE. These accelerators will widen the range of potential applications, especially when deployed in cloud server environments.

A common question in deployment of cryptography currently, is "What about the threat from Quantum Computers?" Interestingly, the technology behind modern HE is exactly the same technology that is behind the proposals for quantum resistant cryptography. Indeed, the development of so-called post-quantum cryptography and FHE have gone hand in hand, with an improvement in one often being able to be applied to the other. Thus, even if a quantum computer is just around the corner, the data encrypted using modern HE schemes will still be secure.

41.A 'Beyond-Quantum' Equivalence Principle for Superposition and Entanglement

by Foundational Questions Institute
https://phys.org/news/2022-05-beyond-quantum-equivalence-principle-superposition-entanglement.html

The physics of the microrealm involves two famous and bizarre concepts: The first is that prior to observation, it is impossible to know with certainty the outcome of a measurement on a particle; rather the particle exists in a "superposition" encompassing multiple mutually exclusive states. So a particle can be in two or more places at the same time, and you can only calculate the probability of finding it in a certain location when you look. The second involves "entanglement," the spooky link that can unite two objects, no matter how far they are separated. Both superposition and entanglement are described mathematically by quantum theory. But many physicists believe that the ultimate theory of reality may lie beyond quantum theory. Now, a team of physicists and mathematicians has discovered a new connection between these two weird properties that does not assume that quantum theory is correct. Their study appears in Physical Review Letters.

"We were really excited to find this new connection that goes beyond quantum theory because the connection will be valid even for more exotic theories that are yet to be discovered," says Ludovico Lami, a member of the physics think-tank, the Foundational Questions Institute, FQXi, and a physicist at the University of Ulm, in Germany. "This is also important because it is independent of the mathematical formalism of quantum theory and uses only notions with an immediate operational interpretation," he adds. Lami co-authored the study with Guillaume Aubrun of Claude Bernard University Lyon 1, in France, Carlos Palazuelos, of the Complutense University of Madrid, in Spain, and Martin Plávala,

of Siegen University, in Germany.

While quantum theory has proven to be supremely successful since its development a century ago, physicists have struggled to unify it with gravity to create one overarching "theory of everything." This suggests that quantum theory may not be the final word on describing reality, inspiring physicists to hunt for a more fundamental framework. But any such ultimate theory must still incorporate superposition, entanglement, and the probabilistic nature of reality, since these features have been confirmed time and again in lab tests. The interpretation of these experiments does not depend on quantum theory being correct, notes Lami.

Quantum cryptography

There are practical implications too. Quantum entanglement plays a key role in the design of quantum computers–machines that could outperform standard computers at certain tasks–and in quantum cryptographic protocols, which are already in use and exploit quantum rules to provide ultra-secure communication across channels that, in theory, are immune to hacking. But if quantum theory eventually needs to be replaced by another, more fundamental theory in the future, will we discover that these rules were not really valid or these cryptographic protocols are not secure as promised?

The problem is that to find out you need to analyze superposition and entanglement in terms of some general–and as yet unknown–theory, without using the mathematics of quantum theory. How can you do that? Lami and his colleagues solved this puzzle by studying "general probabilistic theories," rather than quantum theory. The research was supported in part through a grant that Lami and others received from the Foundational Questions Institute, FQXi, to study the hallmarks and limitations of intelligence in generalized probabilistic theories, allowing them to examine how information is processed in abstract classical, quantum, and "beyond quantum" systems. "This FQXi grant gave me the chance to think about some universal features of information processing in theories beyond quantum mechanics, mathematically modeled by general probabilistic theories, more closely," says Lami. "And the cryptographic primitive example that we study, secret key distribution, is one of the simplest tasks where this formalism can be applied."

In the new paper, published in Physical Review Letters, the team has shown that two physical theories exhibit entanglement when combined, if and only if they both exhibit local superpositions. This means that entanglement and superposition are equivalent in any physical theory, not just in quantum theory. They also calculated that in systems where this equivalence holds–whether quantum or beyond-quantum–the laws of the theory can be exploited for ultra-secure encryption. In particular, the team showed that a certain popular quantum cryptographic protocol, known as "BB84," will always work–even if one day it is found that quantum theory is not fully correct, and needs to be replaced with a more fundamental theory.

"It is somehow reassuring to know that cryptography is really a feature of all non-classical theories, and not just a quantum oddity, since many of us believe that the ultimate theory of nature will likely be non-classical," says Lami. "Even if one day we found quantum theory to be incorrect we will still know that secret key distribution can in principle work."

