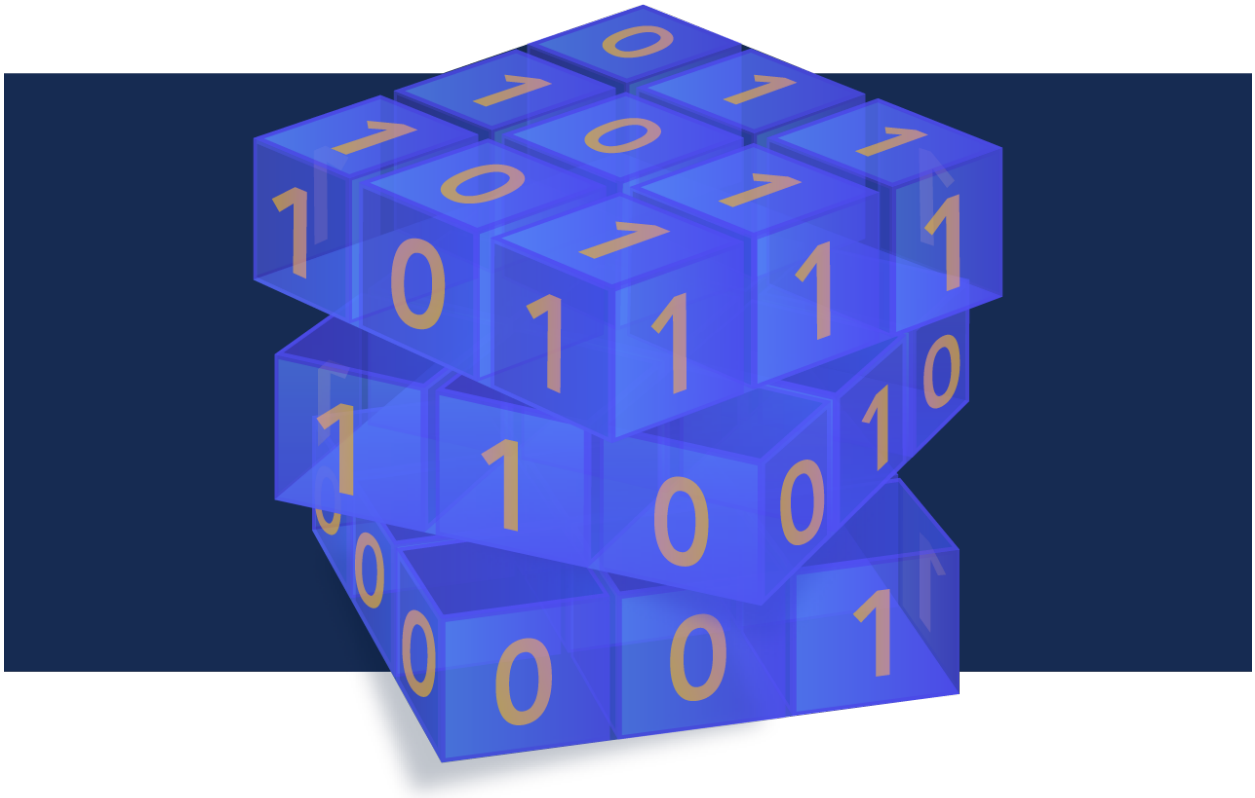
# Crypto News

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

## April 01, 2022



# 1.Editorial

It's officially spring and you know what that means! Warm weather, green grass, and blue skies for all of us! So make the most of it by heading out into the sunshine with this months issue of CryptoNews.

Start with article #30 to learn about how Artificial Intelligence may impact how your organization manages alerts in the future. We all know the importance of not just logging but monitoring system, network, application, etc. alerts regularly. With the average business receiving more than 10,000 alerts per day, the "monitoring" portion can be difficult to do regardless of how big your team is to support such an effort. The first step of course is to properly configure alerting systems from the start to minimize false positives. Once that's managed, perhaps there is more that can be done. How about a way to automate the monitoring aspect using AI? What concerns do you or should you have using AI to complete actions related to monitoring?

For our math lovers, hop on over to article #39. A previously unsolvable mathematical puzzle from 1779 may finally have a solution. How you say? Quantum computers of course! The puzzle introduced by Leonard Euler was proven to be unsolvable in 1900 by Gaston Tarry. But now, a solution for the 6x6 arrangement for Euler's "36 officers" problem is highly probable. Do you have goosebumps yet? I sure do! As always, there are a number of exciting articles throughout this edition that you won't want to miss. Take a look and let us know what other articles caught your eye. 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.Quantum Computers Not a Threat to Bitcoin: MIT Review

by Andrew Throuvalas
https://cryptopotato.com/quantum-computers-not-a-threat-to-bitcoin-mit-review/

Sankar Das Sarma – a physicist from the University of Maryland – recently wrote at length about why the capabilities of quantum computing are overhyped at the moment. Specifically, he clarifies that quantum computing has evolved nowhere close to the stage required to break the public key cryptography used in popular technologies today – such as Bitcoin.

## A Long Way to Go for Quantum Computing

As written in an opinion piece for Technology Review, Sarma suggests that 'Quantum Computing' has become the second most overhyped buzzword next to 'Artificial Intelligence'. Yet despite the substantial investments into quantum R&D from major institutions like Alphabet, Amazon, and Microsoft, it's unlikely they'll be able to produce something of use any time soon.

"Established applications for quantum computers do exist," states Sarma. For example, there's a theoretical application of Quantum computing for finding the prime factors of large numbers exponentially faster than existing schemes. This, he explains, is at the heart of breaking RSA-based cryptography widely used for both email and cryptocurrency transactions.

As such, national governments everywhere have devoted great attention and funding to quantum computing. However, what can be conceptualized in theory isn't always easily built-in practice.

"The most advanced quantum computers today have dozens of decohering (or "noisy") physical qubits," said the professor. These qubits are used primarily for a process called "quantum error correction", which compensates for the fact that quantum states are fast to disappear.

However, a computer that could actually crack RSA would require many millions or even billions of qubits. Only tens of thousands would be used for real computation, while the rest would be used for error correction.

While Sarma calls qubit systems today a "scientific achievement" they cannot yet solve a problem "that anybody cares about."

"It is akin to trying to make today's best smartphones using vacuum tubes from the early 1900s... What is missing is the breakthrough of integrated circuits and CPUs leading to smartphones."

### Bitcoin's Public Key Cryptography

Most cryptocurrencies today use public keys as "crypto addresses" to which any outside party can send their digital assets. However, to send a transaction from that address, one is required to know the private key from which that public key was derived.

While a private key can easily identify a public key it is compatible with, it is currently impossible to decipher a private key just by knowing someone's public key alone.

Nevertheless, not everyone is careful to keep their private keys safe. A hacker managed to steal $600 million in funds from the Ronin network this week by securing the private keys belonging to 5 of 9 validator nodes on the network.

# 3.HSBC Working with IBM to Accelerate Quantum Computing Readiness

by Tineke Dullaart-Mertens and Mark Hadley
https://newsroom.ibm.com/2022-03-29-HSBC-Working-with-IBM-to-Accelerate-Quantum-Computing-Readiness

HSBC and IBM today announced that they will work together on exploring applications for quantum computing in financial services.

The new three-year collaboration is designed to bolster HSBC's expertise in quantum computing and ensure its organizational readiness to take full advantage of the technology.

As part of the agreement, the bank will join the IBM Quantum Accelerator program, giving it access to IBM's premium plan of quantum computing systems, including its recently announced 127-qubit processor, Eagle, as well as IBM's quantum expertise, to help validate and progress potential quantum use cases.

HSBC will explore the use of quantum computing for pricing and portfolio optimisation, to advance its net zero goals, and to mitigate risks, including identifying and addressing fraudulent activity. The bank will upskill colleagues in quantum technology through internal training programmes, as well as actively recruiting quantum computing research scientists, to build a dedicated capability within its innovation team.

Colin Bell, Chief Executive Officer, HSBC Bank plc and HSBC Europe, said: "By investing in quantum computing we are innovating for the future, to make banking easier for our customers. This technology has the potential to transform how we run areas of the bank by addressing challenges which classical computers may never be able to solve, alone. Our work with IBM, a leading provider of quantum computing, is essential to harnessing this potentially game-changing technology for financial services."

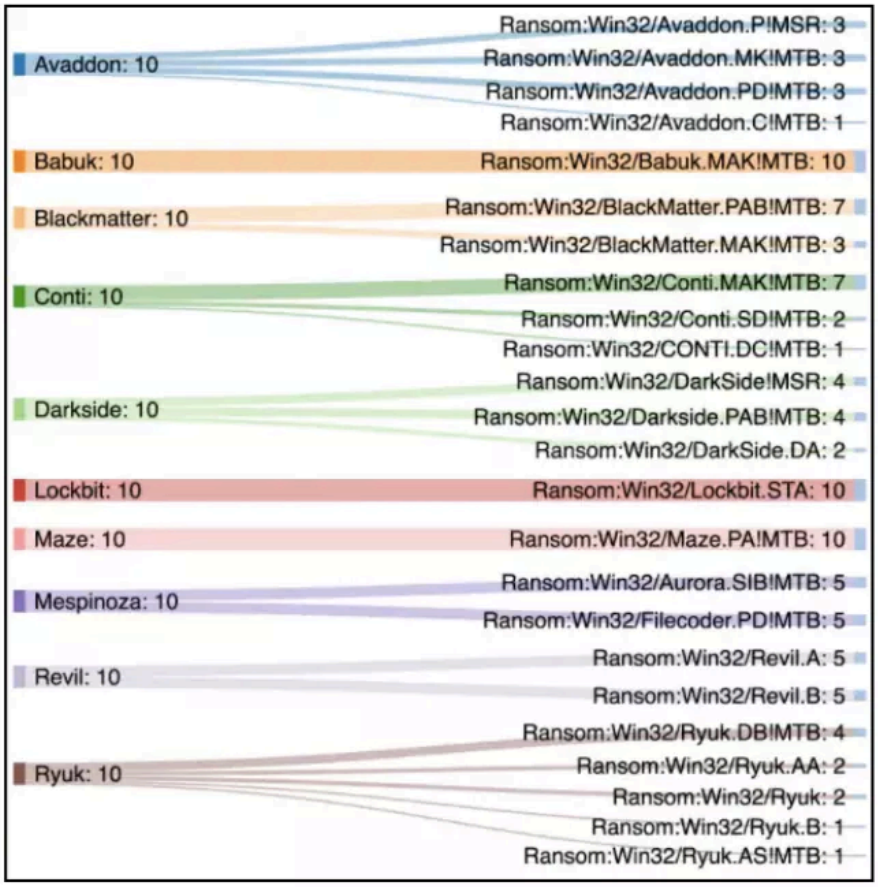
"Financial institutions and organizations around the world are eagerly awaiting real-world applications of quantum computing and exploring industry applications for quantum computing should be a key tenet of any enterprise strategy today," said Dr. Darío Gil, Senior Vice President and Director of IBM Research. "We are excited to team with HSBC to explore applications of quantum technology to their business operations and help turn their aspirations into reality."

A recent report from IBM's Institute for Business Value, **The Quantum Decade**, delineates how the exponential power of quantum computing could dramatically reshape the way financial institutions and other organizations tackle their most pressing challenges in a post-pandemic world with a discovery-driven approach that may spur new hyper-automated and deeply integrated business models.

More than 175 clients, including Fortune 500 companies, start-ups, academic institutions and research labs, work with IBM Quantum technology to advance quantum computing and explore practical applications. The IBM Quantum team and clients are researching and exploring how quantum computing will help a variety of industries and disciplines, including finance, energy, chemistry, materials science, optimization and machine learning, among many others.

# 4.Fastest Ransomware Found to Encrypt 53GB of Data in Just Over Four Minutes




| Family | Median Duration |
|---|---|
| LockBit | 00:05:50 |
| Babuk | 00:06:34 |
| Avaddon | 00:13:15 |
| Ryuk | 00:14:30 |
| Revil | 00:24:16 |
| BlackMatter | 00:43:03 |
| Darkside | 00:44:52 |
| Conti | 00:59:34 |
| Maze | 01:54:33 |
| Mespinoza (PYSA) | 01:54:54 |
| **Average of the median** | **00:42:52** |

by Humza Aamir
https://www.techspot.com/news/93944-fastest-ransomware-found-encrypt-53gb-data-over-four.html

For IT admins and cybersecurity teams, a ransomware attack is a crucial race against time to detect and contain damage while salvaging what's left of a company's data assets. But how much reaction time is there when such an incident occurs? Not a lot it seems, as revealed by ransomware testing of ten candidates, where LockBit led the pack by encrypting nearly 100,000 files on a Windows Server machine in just over four minutes.

The ransomware encryption speed test conducted by Splunk involved ten samples from ten ransomware families, which were run on four different 'victim' profiles. From a total of 400 test runs, a sample from LockBit running on a Windows Server 2019 machine emerged as the fastest ransomware, encrypting all 53GB of test data in just four minutes and nine seconds.

This test data consisted of 98,561 files, comprising pdfs, and excel and word documents. Meanwhile, the ransomwares were tested on a Windows 10 and Windows Server 2019 machine and included samples from REvil, Darkside, Babuk, Maze, LockBit, and several others. LockBit not only had the fastest sample, but also came out first overall in terms of median duration.

The interestingly named 'Babuk' ransomware emerged second overall, though it had its reputation spoiled somewhat by having the slowest individual sample that took over three and a half hours for file encryption.

Splunk also shared a whitepaper, offering a comprehensive look at this research. As for strategies to adopt in case of a ransomware attack, the company advises using multi-factor authentication, network segmentation, centralized logging, and keeping systems patched.

# 5.KT Partners with Toshiba Digital Solutions for Quality Evaluation of Hybrid Quantum Cryptography Communication

by Lim Chang-won
https://www.ajudaily.com/view/20220328105424271

In cooperation with its Japanese partners, KT, a major telecom company in South Korea, will carry out the quality evaluation of hybrid quantum cryptography communication using equipment from different manufacturers on a long-distance test network between Seoul and the southern port city of Busan.

Hybrid quantum cryptography communication was implemented between Seoul and Busan, using domestic equipment and technology from Toshiba Digital Solutions, a Japanese company that provides system integration services, and software solutions. It is the first time in the world to implement hybrid quantum cryptography communication in long-distance sections.

In the 5G era, the importance of cybersecurity in mobile communications will rise exponentially. Quantum cryptography has emerged as an essential solution for safeguarding critical information be-

cause it is impossible to copy data encoded in a quantum state. South Korean companies have tried to lead the standardization of quantum cryptographic communication technology.

"We will continue research, development and investment to implement quantum Internet, not just quantum cryptography communication," KT's convergence technology lab head Kim Yi-han said in a statement on March 28. For the quality evaluation that will last until April 15, KT will utilize its quantum cryptography service quality parameter, which was approved in February by the International Telecommunication Union (ITU), an international telecommunication technology standardization governing body.

KT and Toshiba Digital Solutions would operate an open QKDaaS testbet for two years from the second quarter of 2022 to expand a quantum industry ecosystem at home and abroad. The testbed operates in a section between Seoul and Daejeon to support the evaluation of quantum cryptography communication technology and the development of next-generation application services.

Quantum key distribution (QKD) is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics. QKD as a service (QKDaaS) is a subscription-type service in which a business operator builds quantum cryptography communication facilities and provides only quantum cryptography keys to customers.

KT said the testbed would enable technological cooperation between domestic and foreign quantum cryptography communication companies, provide a better test environment for equipment manufacturers, and increase the competitiveness of domestic technologies.

# 6.CISA Adds 66 Vulnerabilities to List of Bugs Exploited in Attacks

by Bill Toulas
https://www.bleepingcomputer.com/news/security/cisa-adds-66-vulnerabilities-to-list-of-bugs-exploited-in-attacks/

The Cybersecurity and Infrastructure Security Agency (CISA) has added a massive set of 66 actively exploited vulnerabilities to its catalog of 'Known Exploited Vulnerabilities.'

These flaws have been observed in real cyberattacks against organizations, so they are published to raise awareness to system administrations and serve as official advisories for applying the corresponding security updates.

In this case, CISA gives federal agencies until April 15, 2022, to patch the listed vulnerabilities and reduce the risk of falling victim to cyberattacks.

## A massive 66 vulnerabilities

The new set of 66 actively exploited vulnerabilities published by CISA spans disclosure dates between 2005 and 2022, covering a broad spectrum of software and hardware types and versions.

The Mitel CVE-2022-26143 and Windows CVE-2022-21999 vulnerabilities disclosed in February are two particularly interesting bugs.

Microsoft fixed the CVE-2022-21999 Windows Print Spooler bug in the February 2022 Patch Tuesday updates, and threat actors had not actively exploited it at the time. The vulnerability allows attackers to achieve code execution as SYSTEM, the highest Windows privileges when exploited.

The Mitel CVE-2022-26143 bug affects devices using a vulnerable driver (TP-240), including MiVoice Business Express and MiCollab.

This flaw allows a record-breaking DDoS amplification ratio of about 4.3 billion to 1, using a method of internal reflection.

Akamai, the company that discovered the Mitel bug, has already reported attacks in the wild beginning last February, targeting governments, financial institutions, and internet service providers.

Additionally, the set contains a 2005 RCE flaw on Hewlett Packard OpenView, a 2009 buffer overflow on Adobe Reader and Acrobat, a 2009 RCE on phpMyAdmin, and another 23 flaws dating between 2010 and 2016.

The addition of these 66 vulnerabilities at this time doesn't necessarily mean that CISA's analysts just spotted their active exploitation in the wild.

Quite possibly, the agency is publishing new sets with intervals between them to not overwhelm system administrators, striving for a balance between practical constraints and best security practices.

Another possible explanation for the addition of such old vulnerabilities in the catalog could be that they're leveraged in new exploit chains that are applicable today, suddenly transcending from obsolescence to relevance.

However, the list shows us how quickly threat actors begin targeting a vulnerability once a vendor discloses it.

For example, the Windows Print Spooler CVE-2022-21999 vulnerability, the Mitel DDoS CVE-2022-26143 amplification vulnerability, and the CVE-2022-26318 WatchGuard vulnerabilities were disclosed in February and were quickly exploited by threat actors.

Due to this, it is critical for admins to apply security updates as soon as possible to prevent their exploitation, especially on internet-exposed devices.

Due to the large number of flaws comprising the latest set, CISA hasn't supplied the usual summary table, so system administrators will have to review the new entries on the catalog, which now counts a total of 570 vulnerabilities.

Once at the catalog, you can click on the 'Date Added' column header to sort by the most recently added vulnerabilities.

# 7.Scientists Work to Turn Noise on Quantum Computers to Their Advantage

by Louise Lerner
https://scitechdaily.com/scientists-work-to-turn-noise-on-quantum-computers-to-their-advantage/

Scientists simulate 'fingerprint' of noise on quantum computer. Unique study could point way to new approach, uses for quantum technology.

For humans, background noise is generally just a minor irritant. But for quantum computers, which are very sensitive, it can be a death knell for computations. And because "noise" for a quantum computer increases as the computer is tasked with more complex calculations, it can quickly become a major obstacle.

But because quantum computers could be so incredibly useful, researchers have been experimenting with ways to get around the noise problem. Typically, they try to measure the noise in order to correct for it, with mixed success.

A group of scientists from the University of Chicago and Purdue University collaborated on a new technique: Instead of directly trying to measure the noise, they instead construct a unique "fingerprint" of the noise on a quantum computer as it is seen by a program run on the computer.

This approach, they say, shows promise for mitigating the noise problem—as well as suggesting ways that users could actually turn noise to their advantage.

"We wondered if there was a way to work with the noise, instead of against it," said David Mazziotti, professor in the Department of Chemistry, James Franck Institute and the Chicago Quantum Exchange and a co-author on the study, which was published in Nature Communications Physics.

## 'A fresh approach'

Quantum computers are based on the laws of how particles behave at the atomic level. Down at that level, particles obey a set of very strange rules; they can be in two different states at once, or become 'entangled' across space. Scientists hope to harness these abilities as the basis for computers.

In particular, many scientists want to use quantum computers to better understand the rules of the natural world, because molecules operate according to the laws of quantum mechanics—which should theoretically be easier to simulate using a quantum computer.

But despite significant advances in quantum computing technology over the past decade, computational ability has lagged behind scientists' hopes. Many had assumed that increasing the number of computer bits—"qubits," for quantum computers—would help alleviate the noise problem, but since noise limits accuracy, scientists still haven't been able to perform many of the computations they would like.

"We thought it might be time for a fresh approach," said co-author Sabre Kais, professor of physics and chemistry at Purdue University.

To date, scientists have tried to understand the effect of noise by directly measuring the noise in each qubit. But cataloging such discrete changes is difficult, and, the group thought, perhaps not always the most efficient route.

"Quite often in physics, it is actually easier to understand the overall behavior of a system than to know what each part is doing," said co-author Zixuan Hu, a postdoctoral researcher at Purdue. "For example, it is hard to simulate what each molecule in a glass of water is doing, but it is much easier to predict the behavior of the whole."

So instead of trying to precisely measure the actual noise, the scientists decided to run a test to get a sense of the overall noise that quantum computers experience.

They picked a particular computation of a molecule displaying quantum behavior, and ran it as a simulation on a quantum computer. Then they tweaked the settings on the problem in several different directions, and kept track of how the noise responded. "By putting this all together, we build a 'fingerprint' of the noise as perceived by the simulation that we're running," said Mazziotti.

Hu explained that running a computation of a molecule that is already well known helped them tease out the specific effects of the noise.

"We know very little about quantum computers and noise, but we know really well how this molecule behaves when excited," said Hu. "So we use quantum computers, which we don't know much about, to mimic a molecule which we are familiar with, and we see how it behaves. With those familiar patterns we can draw some understanding."

This operation gives a more 'bird's-eye' view of the noise that quantum computers simulate, said Scott Smart, a Ph.D. student at the University of Chicago and first author on the paper.

The authors hope this information can help researchers as they think about how to design new ways to correct for noise. It could even suggest ways that noise could be useful, Mazziotti said.

For example, if you're trying to simulate a quantum system such as a molecule in the real world, you know it will be experiencing noise—because noise exists in the real world. Under the previous approach, you use computational power to add a simulation of that noise.

"But instead of building noise in as additional operation on a quantum computer, maybe we could actually use the noise intrinsic to a quantum computer to mimic the noise in a quantum problem that is difficult to solve on a conventional computer," Mazziotti said.

The authors believe this unique approach to the noise problem is helpful as researchers continue to explore the young field of quantum computing.

"We're still not even sure what kinds of problems for which quantum computers will be most useful," Mazziotti said. "We hope this will provide a different way to think about noise that will open up new avenues for simulating molecules with quantum devices."

# 8.The Zprize Competition for Zero Knowledge Cryptography by Aleo

by Alex R
https://hackernoon.com/announcement-the-zprize-competition-for-zero-knowledge-cryptography-by-aleo

Zero-knowledge cryptography has gone from being an academic curiosity to a cutting-edge technology providing solutions to real-world problems within the last decade. From the launch of ZCash in 2016 to enable private money, zero-knowledge proofs are increasingly viewed as the key solution to resolving issues with scalability and privacy on Ethereum and beyond.

These solutions have been enabled by the incredible progress across the field. First of all, better algorithms and better implementations have made zero-knowledge proof generation faster than ever.

Over five years ago, generating a single zero-knowledge proof in ZCash took around 60 seconds on a laptop. Fast forward to today, networks such as Filecoin and Aleo's testnet have provers generating tens of thousands of proofs per second, an improvement of several orders of magnitude.

In addition, new families of universal proof systems such as Marlin, PLONK, and Halo2 enable more general programmability and flexibility for programs. Although there has been significant progress, there are still challenges to overcome to attain widespread adoption.

These challenges include high computational costs of generating proofs. Just as TLS and encryption on the internet took off after basic encryption algorithms such as AES were integrated directly into modern processors, we believe zero-knowledge cryptography will only become practical at scale with hardware acceleration.

## What is the ZPrize Competition?

On March 28th, Aleo will be partnering with other members of the industry to launch the ZPrize competition where participants will compete for over $2 million of cash prizes.

The goal of ZPrize is to bring together the best teams at the intersection of research and engineering, hardware and software to create the fastest, most efficient provers and/or verifiers for different

applications/hardware platforms.

Through this initiative, we are going all-in on zero-knowledge cryptography to solve the scalability and privacy problems facing Web 3 today. During this competition, participants will have the opportunity to meet and collaborate with leaders in the industry, including the Ethereum Foundation, ZCash Foundation, Mina, Aztec.

Participating projects will have the opportunity to sponsor prizes directly relevant to their specific protocols and applications. To start things off, Aleo is committing $2M and up to 8M Aleo Credits (the future token of our decentralized network) to the prize pool.

### Important Dates

On March 28th, we will be accepting applications to participate in the competition[1].

- Application Submissions: **March 28th - April 21st.**
- Project Submission Date: **August 1st.**
- ZPrize Winners' Announcement: **August 8th.**

# 9.Israel's First Quantum Computer — a Trapped Ion Device — Launched

by Matt Swayne
https://thequantuminsider.com/2022/03/25/israels-first-quantum-computer-a-trapped-ion-device-launched/

Building a working quantum computer is such a daunting venture that many believe it's only for tech giants and superpowers, something on a scale beyond Israel's reach. Prof. Roee Ozeri of the Weizmann Institute of Science begs to differ: "One of the world's first computers, WEIZAC, was built here in the 1950s, when all Israel had was swamps and camels.

Today, Israel is a technological empire; there's no reason we shouldn't be front-runners in the quantum computing race."

In a project reported today in PRX Quantum, Ozeri's team succeeded in building a quantum computer – one of about 30 such machines in the world, and one of less than 10 to rely on an advanced technology known as ion traps. An even larger computer is already in the works in Ozeri's lab, and this one already has a name: In a tribute to WEIZAC, inaugurated at Weizmann back in 1955, the scientists plan to call it WeizQC.

Quantum computers promise to reach computational complexity that is unthinkable using even the

[1] In order to participate in this competition, all submissions must be open-sourced.

most powerful classical computers. This level of ability is known as the "quantum advantage." It should bring about a slew of applications, from designing unbreakable codes and predicting market fluctuations to accelerating the development of new drugs, materials and artificial intelligence systems. That's because in contrast to today's computers, which are limited by the boundaries of classical physics, quantum computers obey an entirely different set of laws – those of quantum mechanics, which rule the microscopic world.

In our familiar world, humans, cats or even bits, the basic units of information in classical computing, can only be in one place at a time. In contrast, quantum bits, known as qubits, can be simultaneously present in more than one position or state, which enables them to conduct multiple calculations in parallel, opening the door to vast computing power.

Ozeri became a pioneer of quantum computing research in Israel some 15 years ago after returning from the United States, where he had conducted his postdoctoral studies under the guidance of Nobel laureate David Wineland.

"Then, quantum computing was done in university labs," Ozeri says. "But in the past decade, commercial companies such as Google, Amazon and IBM joined the race to build a quantum computer, while the United States, China and the European Union initiated massively funded strategic programs to advance the field."

Despite this expansion of research, substantial challenges remain. One of the greatest obstacles is the extreme sensitivity of quantum computers to environmental noise, which stands in the way of building large, complex systems. In a project led by Dr. Tom Manovitz and research student Yotam Shapira, Ozeri's team addressed this challenge by introducing two innovations, both successfully implemented in the quantum computer the researchers have built in their lab.

## Watch out, it's a trap

Today's computers all rely on the same basic hardware, but in the field of quantum computing, several different technologies still compete for top ranking. Among the leading contestants are ion traps, systems in which each ion – that is, each electrically charged atom – represents a single qubit. Just as regular bits can move between two states, 0 and 1, so ion-based qubits can switch between different states, defined by different flight paths of an electron around the atomic nucleus. Instead of standard electronics, qubit switching in an ion trap is done with lasers. These qubit-based operations are called logic gates. Complex computations require gates involving more than one qubit, but such operations are sensitive, and even the tiniest environmental noise will cause the system to lose its quantum nature. To prevent this from happening, the Weizmann researchers developed a pattern of laser pulses that keeps the logic gates robust and stable.

Yet even when the gates are robust, the system's high sensitivity can cause it to accumulate errors that threaten to undo its quantum nature. To correct an error, one must first find it, a task that requires measuring the qubits. But there is a catch: Measuring constitutes an invasive act that inevitably leads to the loss of the system's quantum nature. The solution is to measure only some of the qubits, not all. In trapped-ion-based computers, the measurements are performed by illuminating the ions and determining the states of the qubits by the resulting, if any, scattering of light. In their new

computer, the Weizmann scientists replaced the light detectors that capture the states of individual ions with a camera-based array that detects all the qubits simultaneously. Then, to protect the system's quantum nature, they concealed some of the qubits from the camera. They also developed a way to overcome the slow-down in data processing that had been associated with camera-based arrays: They added electronic circuits that rapidly read out and process the cameras' information, speeding up error correction.

The Weizmann computer is a five-qubit machine, roughly the level achieved by IBM's version when the company first started offering quantum computing as a cloud service. WeizQC, which is currently being built in Ozeri's lab, is scheduled to work with 64 qubits. It is expected to demonstrate the quantum advantage, which until now has only been achieved by computers built in two labs: at Google and at the University of Science and Technology of China.

Project participants included research student Lior Gazit, Dr. Nitzan Akerman and other students and scientists from Ozeri's lab in Weizmann's Physics of Complex Systems Department. Theoretical research accompanying the project was conducted by Prof. Ady Stern of Weizmann's Condensed Matter Physics Department.

# 10.CEA and Startup C12 Join Forces to Develop Next-Generation Quantum Computers

by Karine
https://thequantumhubs.com/cea-and-startup-c12-join-forces-to-develop-next-generation-quantum-computers/

CEA, a French key player in research, development and innovation, and C12 Quantum Electronics, a startup focused on developing the next-generation of quantum computers using carbon nanotubes, today announced a partnership to produce the first multi-qubit chips at wafer scale.

Building on the breakthrough of manufacturing quantum chips on 200mm silicon wafers using CMOS processes, C12 is pursuing the next materials leap in quantum computing: using carbon nanotubes to build quantum bits, or qubits, the fundamental building blocks of quantum computers. By combining an ultra-pure material with an easy-to-manufacture semiconductor device, the company is building a scalable and ultra-coherent platform for quantum computing.

In addition, C12 and CEA have demonstrated a world's-first ability to manufacture, with precision and in volume, core components to calibrate, control and read qubits, using standard manufacturing processes. Combined with C12's unique nano-assembly process, this will enable large-scale integration of reliable qubits.

In addition, the collaboration will further investigate integration of innovative materials to optimize

the properties of qubits hosted in carbon nanotubes, and includes continued work on the design and fabrication of multi-qubit chips. A final full prototype is expected in 2024.

C12, a leader in the search for materials breakthroughs for quantum computing, closed a $10 million seed round of funding in June 2021.

# 11.How Can Quantum Computing Change The World?

by Madhurjya Chowdhury
https://www.analyticsinsight.net/how-can-quantum-computing-change-the-world/

There's a reason why Microsoft, Google, IBM, and Governments across the globe keep making large investments in quantum computing; they expect it will revolutionize the world by addressing issues that today's conventional computers can't solve.

Every industry will be affected by quantum computing. They will alter the way business is done and the security systems in place which protect data, how we battle illnesses and create new materials, as well as how we tackle health and climate challenges.

As the race to build the first commercially functional quantum computer heats up, here we discuss a handful of the ways quantum computing will alter our world.

## Online security

When quantum computers become widely used, there will be both good and terrible consequences for internet security. Our present data encryption methods will be rendered obsolete. Most internet security measures now rely on the fact that "cracking the code" takes an inordinate amount of time as computers crunch big numbers. Quantum computers, on the other hand, will be able to handle this information swiftly, leaving our computers, financial firms, and private information exposed. The good news is that great progress has been made in the development of quantum encryption technologies like quantum key distribution, an ultra-secure communication technique that uses a key to decrypt a message. If the communication is intercepted, no one can read it due to the unusual features of quantum physics.

## Artificial intelligence

Quantum computing is well adapted to processing information, required to enhance machine learning. Quantum computers can evaluate massive amounts of data in order to give artificial intelligence robots the feedback they need to enhance performance. Quantum computers can interpret data far more effectively than ordinary computers, resulting in a shorter learning curve for artificial intelligence robots. Artificial intelligence devices driven by quantum computing insights, like humans, can learn through experience and self-correct. Quantum computers will let AI spread to many sectors

and technology become much more sensible in a very short period of time.

### Drug development

To create an effective drug, chemists must examine the interactions between atoms, proteins, and chemicals to determine whether medicines will improve certain circumstances or cure diseases. This is time and labour expenses due to the large number of combinations that should be examined. Because quantum computers can examine many molecules, proteins, and chemicals at the same time, they allow scientists to identify promising therapeutic possibilities more quickly. Furthermore, certain medications are being withdrawn from clinical trials despite the fact that they may be effective in a portion of the population. Quantum computing will allow a person's DNA to be sequenced and processed considerably faster than current technologies, allowing for individualized medicine creation.

### Traffic control

Quantum computers will be able to swiftly determine the ideal routes concurrently, allowing for more effective scheduling and reducing traffic congestion. Quantum computers are also useful for improving supply chains, fleet operations, air traffic control, and deliveries for pretty much the same reasons.

### Improve weather predictions

Since quantum computers can examine all the data simultaneously, meteorologists will have a far better idea of adverse weather conditions, allowing them to warn people and ultimately save lives, pain, and money. We will also acquire a better understanding of how we are impacting our environment since quantum computers will aid in the development of better climate models.

## 12.Entrust Helps Enterprises Prepare Now for Post Quantum Security Journey With New PQ Testing and Development Solutions

by Business Wire
https://www.benzinga.com/pressreleases/22/03/b26277625/entrust-helps-enterprises-prepare-now-for-post-quantum-security-journey-with-new-pq-testing-and-de

New suite of PQ testing and development toolkits, services, and cryptographic consulting help enterprises to bring crypto agility and resilience into their organizations today to get ready for the post quantum world

Entrust, a leading provider of trusted identities, payments, and data protection solutions, has announced four new solutions aimed at helping organizations prepare for the security challenges and opportunities presented by quantum computers.

While not powerful enough to do so today, advances in quantum computing threaten the integrity of traditional asymmetric encryption algorithms, with the potential to empower brute force attacks that will succeed in minutes rather than years. Post quantum (PQ) cryptography is the development of new cryptographic approaches that can be implemented using today's computers, but will be impervious to attacks from tomorrow's quantum ones.

The NIST has published a short-list of PQ safe algorithms which will be resilient to these attacks. Although these algorithms are undergoing review from academics and industry, security-conscious organizations need to start work now in order to be fully prepared for a post quantum future. This includes carrying out due diligence by investigating the adoption of the short-listed algorithms in their cryptographic ecosystem.

To help organizations start preparing for this future now, Entrust is making available four new products designed to help organisations to assess their cryptographic stance and integrate quantum resistant algorithms into their encryption workflows and services. The new offerings are:

## Cryptographic Center of Excellence Expands to Support PQ Preparedness

The Entrust Cryptographic Center of Excellence consulting portfolio - which provides actionable recommendations to remediate identified risks in crypto systems – is evolving to help organisations prepare to manage the challenges of PQ. The upcoming updates to the Crypto Agility Maturity Assessment will help organizations identify their readiness to manage the introduction of PQ algorithms and provide a roadmap to achieve the required level of crypto agility.

## Entrust nShield Post Quantum Cryptography Option Pack

For customer wishing to prepare for a PQ world and are looking to evaluate the use of NIST PQ shortlisted algorithms running within a representative Entrust nShield Hardware Security Module (HSM) environment, Entrust offers an advanced preview of a new option pack that provides a software development suite of cryptographic functions based on NIST PQ shortlisted algorithms running within a representative Entrust nShield Hardware Security Module (HSM) environment. This sandbox environment supports a range of PQ cryptographic operations including key generation, encrypt, decrypt, sign, verify and key exchange. It enables developers to test PQ algorithms, invoke crypto operations via Java calls and execute code within a secure test environment underpinned by a quantum safe root of trust.

## Quantum Java Toolkit

Available as a beta release, this pluggable Java toolkit provides a way for organizations to integrate quantum safe algorithms into their digital certificate generation workflows. It is being made available to organizations who want to start building secure applications with PQ cryptography and supports

composite certificate draft standards and traditional single algorithm certificates. Entrust has developed this toolkit to support the National Institute of Standards and Technology (NIST) post quantum development and is a round 3 signature finalist in the NIST competition.

### PKIaaS for Post Quantum

In a PQ environment, Public Key Infrastructure (PKI) providers will need to issue hybrid or composite certificates combining classical and quantum safe algorithms. By providing a cloud-based PKI as a Service offering, Entrust can provide customers with composite and pure quantum Certificate Authority hierarchies. PQ via PKIaaS is expected to be available to applicants as a beta in April 2022 and will give organizations the ability to test multi-certificates or composite certificates with their applications, with the added benefit that these will be underpinned by Entrust nShield HSMs.

"Post-quantum computing is an inevitable threat to cybersecurity. While it is unclear when exactly the post-quantum threat will become real, it is generally expected to occur within the decade. The migration to quantum-safe algorithms can take several years, so the time to prepare for post-quantum is now," said Anudeep Parhar, Chief Information Officer at Entrust. "Entrust is at the forefront of post-quantum cryptography. We are participating members of the Internet Engineering Task Force (IETF), and we are also participants in the NIST PQ competition. Through growth initiatives and investment in solutions like those announced today, we are helping our customers today to prepare for tomorrow."

# 13.Making Quantum Computing More Resilient to Noise

by Karine
https://thequantumhubs.com/making-quantum-computing-more-resilient-to-noise/

Researchers at MIT are working to mitigate the noise problem in quantum computing by developing a technique that makes the quantum circuit itself resilient to noise. (Specifically, these are "parameterized" quantum circuits that contain adjustable quantum gates.) The team created a framework that can identify the most robust quantum circuit for a particular computing task and generate a mapping pattern that is tailored to the qubits of a targeted quantum device.

Their framework, called QuantumNAS (Noise Adaptive Search), is much less computationally intensive than other search methods and can identify quantum circuits that improve the accuracy of machine learning and quantum chemistry tasks. When the researchers used their technique to identify quantum circuits for real quantum devices, their circuits outperformed those generated using other methods.

The researchers focused on variational quantum circuits, which use quantum gates with trainable parameters that can learn a machine learning or quantum chemistry task. To design a variational quantum circuit, typically a researcher must either hand-design the circuit or use rule-based methods to design the circuit for a particular task, and then try to find the ideal set of parameters for each

quantum gate through an optimization process.

With QuantumNAS, the researchers seek to reduce the overall search and training cost while identifying the quantum circuit that contains the ideal number of parameters and appropriate architecture to maximize accuracy and minimize noise.

To do that, they first design a "SuperCircuit," which contains all the possible parameterized quantum gates in the design space. That SuperCircuit will be used to generate smaller quantum circuits that can be tested.

They train the SuperCircuit once, and then because all other candidate circuits in the design space are subsets of the SuperCircuit, they inherit corresponding parameters that have already been trained. This reduces the computational overhead of the process.

Once the SuperCircuit has been trained, they use it to search for circuit architectures that meet a targeted objective, in this case high robustness to noise. The process involves searching for quantum circuits and qubit mappings at the same time using what is known as an evolutionary search algorithm.

This algorithm generates some quantum circuit and qubit mapping candidates, then evaluates their accuracy with a noise model or on a real machine. The results are fed back to the algorithm, which selects the best performing parts and uses them to start the process again until it finds the ideal candidates.

# 14.Single-Photon Source Paves the Way for Practical Quantum Encryption

by The Optical Society
https://phys.org/news/2022-03-single-photon-source-paves-quantum-encryption.html

Researchers have developed a new high-purity single-photon source that can operate at room temperature. The source is an important step toward practical applications of quantum technology, such as highly secure communication based on quantum key distribution (QKD).

"We developed an on-demand way to generate photons with high purity in a scalable and portable system that operates at room temperature," said Helen Zeng, a member of the research team from the University of Technology Sydney in Australia. "Our single-photon source could advance the development of practical QKD systems and can be integrated into a variety of real-world quantum photonic applications."

In the Optica Publishing Group journal Optics Letters, Zeng and colleagues from Australia's University of New South Wales and Macquarie University describe their new single-photon source and show that it can produce over ten million single photons per second at room temperature. They also incor-

porated the single-photon source into a fully portable device that can perform QKD.

The new single-photon source uniquely combines a 2-D material called hexagonal boron nitride with an optical component known as a hemispherical solid immersion lens, which increases the source's efficiency by a factor of six.

## Single photons at room temperature

QKD offers impenetrable encryption for data communication by using the quantum properties of light to generate secure random keys for encrypting and decrypting data. QKD systems require robust and bright sources that emit light as a string of single photons. However, most of today's single-photon sources don't perform well unless operated at cryogenic temperatures hundreds of degrees below zero, which limits their practicality.

Although hexagonal boron nitride has previously been used to create a single-photon source that operates at room temperature, until now researchers had not been able to achieve the efficiency needed for real-world application. "Most approaches used to improve hexagonal boron nitride single-photon sources rely on precisely positioning the emitter or using nano-fabrication," said Zeng. "This makes the devices complex, difficult to scale and not easy to mass produce."

Zeng and colleagues set out to create a better solution by using a solid immersion lens to focus the photons coming from the single-photon emitter, allowing more photons to be detected. These lenses are commercially available and easy to fabricate.

The researchers combined their new single-photon source with a custom-built portable confocal microscope that can measure the single photons at room temperature, creating a system that can perform QKD. The single-photon source and confocal microscope are housed inside a robust package that measures just 500 x 500 millimeters and weighs around 10 kilograms. The package is also engineered to deal with vibration and stray light.

"Our streamlined device is easier to use and much smaller than traditional optical table setups, which often take up entire labs," said Zeng. "This allows the system to be used with a range of quantum computing schemes. It could also be adapted to work with existing telecommunications infrastructure."

## Demonstrating quantum cryptography

Tests of the new single-photon source showed that it could achieve a single-photon collection rate of $10^7$ Hz while maintaining excellent purity — meaning each pulse had a low probability of containing more than one photon. It also showed exceptional stability over many hours of continuous operation. The researchers also demonstrated the system's ability to perform QKD under realistic conditions, showing that secured QKD with 20 MHz repetition rates would be feasible over several kilometers.

Now that the researchers have established proof that their portable device can perform complex quantum cryptography, they plan to perform further testing of its robustness, stability, and efficiency during encryption. They also plan to use the new source to perform QKD in real-world conditions,

rather than inside the lab. "We are now ready to transform these scientific advances in quantum 2-D materials into technology ready products," said Igor Aharonovich, who led the project.

# 15.New World Record for Qubit Storage

by Julien-Levallois
https://www.swissquantumhub.com/new-world-record-for-qubit-storage/

Computers, smartphones, GPS: quantum physics has enabled many technological advances. It is now opening up new fields of research in cryptography (the art of coding messages) with the aim of developing ultra-secure telecommunications networks. There is one obstacle, however: after a few hundred kilometers within an optical fiber, the photons that carry the qubits or 'quantum bits' (the information) disappear. They therefore need 'repeaters', a kind of 'relay', which are partly based on a quantum memory. By managing to store a qubit in a crystal (a «memory») for 20 milliseconds, a team from the University of Geneva (UNIGE) has set a world record and taken a major step towards the development of long-distance quantum telecommunications networks. This research can be found in the journal npj Quantum Information.

Developed during the 20th century, quantum physics has enabled scientists to describe the behavior of atoms and particles as well as certain properties of electromagnetic radiation. By breaking with classical physics, these theories generated a real revolution and introduced notions without equivalent in the macroscopic world such as superposition, which describes the possibility for a particle to be in several places at once, or entanglement, which describes the ability of two particles to affect each other instantaneously even at a distance ('spooky action at a distance').

Quantum theories are now at the heart of much research in cryptography, a discipline that brings together techniques for encoding a message. Quantum theories make it possible to guarantee perfect authenticity and confidentiality for information (a qubit) when it is transmitted between two interlocutors by a particle of light (a photon) within an optical fiber. The phenomenon of superposition let the sender know immediately whether the photon conveying the message has been intercepted.

## Memorizing the signal

However, there is a major obstacle to the development of long-distance quantum telecommunication systems: beyond a few hundred kilometers, the photons are lost and the signal disappears. Since the signal cannot be copied or amplified – it would lose the quantum state that guarantees its confidentiality – the challenge is to find a way of repeating it without altering it by creating 'repeaters' based, in particular, on a quantum memory.

In 2015, the team led by Mikael Afzelius, a senior lecturer in the Department of Applied Physics at the Faculty of Science of the University of Geneva (UNIGE), succeeded in storing a qubit carried by a photon for 0.5 milliseconds in a crystal (a 'memory'). This process allowed the photon to transfer its quantum state to the atoms of the crystal before disappearing. However, the phenomenon did not last long enough to allow the construction of a larger network of memories, a prerequisite for the devel-

opment of long-distance quantum telecommunications.

## Storage record

Today, within the framework of the European Quantum Flagship program, Mikael Afzelius' team has managed to increase this duration significantly by storing a qubit for 20 milliseconds. "This is a world record for a quantum memory based on a solid-state system, in this case a crystal. We have even managed to reach the 100 millisecond mark with a small loss of fidelity", enthuses the researcher. As in their previous work, the UNIGE scientists used crystals doped with certain metals called 'rare earths' (europium in this case), capable of absorbing light and then re-emitting it. These crystals were kept at -273.15°C (absolute zero), because beyond 10°C above this temperature, the thermal agitation of the crystal destroys the entanglement of the atoms.

"We applied a small magnetic field of one thousandth of a Tesla to the crystal and used dynamic decoupling methods, which consist in sending intense radio frequencies to the crystal. The effect of these techniques is to decouple the rare-earth ions from perturbations of the environment and increase the storage performance we have known until now by almost a factor of 40," explains Antonio Ortu, a post-doctoral fellow in the Department of Applied Physics at UNIGE. The results of this research constitute a major advance for the development of long-distance quantum telecommunications networks. They also bring the storage of a quantum state carried by a photon to a time scale that can be estimated by humans.

## An efficient system in ten years

However, there are still several challenges to be met. "The challenge now is to extend the storage time further. In theory, it would be enough to increase the duration of exposure of the crystal to radio frequencies, but for the time being, technical obstacles to their implementation over a longer period of time prevent us from going beyond 100 milliseconds. However, it is certain that these technical difficulties can be resolved," says Mikael Afzelius.

The scientists will also have to find ways of designing memories capable of storing more than a single photon at a time, and thus of having 'entangled' photons which will guarantee confidentiality. "The aim is to develop a system that performs well on all these points and that can be marketed within ten years," concludes the researcher.

# 16.Sandbox AQ Is Alphabet's New Bet on The Future of Quantum Cryptography

by Peter Sayer
https://www.cio.com/article/307102/sandbox-aq-is-alphabets-new-bet-on-the-future-of-quantum-cryptography.html

Google's parent Alphabet has spun out a new company, Sandbox AQ, offering enterprises artificial in-

telligence and quantum computing software as a service.

The company is starting life with two major research objectives. The first is the creation of post-quantum cryptosystems and related privacy-enhancing technologies, in an attempt to keep data secure should quantum computing develop to the point of rendering today's encryption techniques obsolete.

The second is the creation of a novel navigation system based on geophysical signals (such as local variations in the earth's magnetic and gravitational fields) rather than satellites. Sandbox AQ suggests such a system could be useful for autonomous vehicles or in areas where access to global navigational satellite systems (GNSSs) is denied. That might have seemed a far-fetched concern until war broke out in Ukraine and the European Union Aviation Safety Agency reported incidents of GPS signal jamming and spoofing around the conflict zone and elsewhere that threatened aircraft navigation.

Sandbox AQ is also looking at the development of new sensors based on quantum phenomena which could be useful in medical diagnostics, and at the discovery of novel materials, including pharmaceuticals, using AI.

Beyond these initial objectives, the company's focus remains vague: It says it intends to apply AI and quantum technology "to develop practical solutions for a broad range of use cases," and to "develop quantum-based applications that do not rely on quantum hardware."

## Crypto customers

The company already claims customers for its cybersecurity offering, including Vodafone Business, the enterprise arm of European mobile operator Vodafone; Japanese operator Softbank Mobile; Mount Sinai Health System, the New York hospital network; and web-hosting company Wix. Others it will be targeting include the US Federal government, critical infrastructure operators, and the financial services industry.

The new company will be led by Jack Hidary, a serial entrepreneur and former New York mayoral candidate. Hidary has worked for Alphabet since 2016, and in 2019 published a college textbook, Quantum Computing: An Applied Approach.

Sandbox AI is still small, with just 55 engineers, scientists, and technologists, but clearly has the ambition to grow rapidly: Its website lists over 30 open positions, most of them in software development and most of them remote.

To fund that growth, it has already landed investments totalling over $100 million from venture capital funds and individuals, including Eric Schmidt, who also serves on its board of directorsSandbox's focus on quantum applications without quantum hardware sounds odd, but developing the hardware is the focus of a team at Google's Quantum AI lab. While companies such as Google, IBM, and Honeywell attempt to build viable quantum computers, there's a thriving market for quantum computing simulation software running with conventional high-performance computing components. Nvidia is targeting this market, as are AWS, Atos, Microsoft, and IBM. And Microsoft and IBM are also working on quantum hardware.

# 17.Explore Azure Quantum's Diverse and Growing Hardware Portfolio for Free

by Fabrice Frachon
https://cloudblogs.microsoft.com/quantum/2022/03/21/explore-azure-quantums-diverse-and-growing-hardware-portfolio-for-free/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Rigetti+March+2022+Newsletter&utm_campaign=Rigetti+March+2022+Newsletter

Azure Quantum is a platform for innovation. There's no better place to experiment and unlock innovation today and prepare the quantum solutions of tomorrow. Last week, we shared the exciting news that we've demonstrated a significant and foundational milestone towards realizing a topological qubit on the path to a scalable quantum machine. And while we're in the early days as an industry, we also know people are eager to expand their quantum computing expertise today and contribute their innovations to a scaled quantum future.

Our rich and growing quantum hardware ecosystem lets you explore and test quantum algorithms and solutions across a diverse range of quantum hardware architectures. And the best news is, you can start exploring leading-edge quantum hardware in Azure Quantum for free. Today, we're thrilled to expand our offerings further by welcoming Pasqal into the Azure Quantum family.

## Pasqal brings neutral-atom quantum technology to Azure Quantum

We unlock new research and innovation capabilities through Azure Quantum with our new partner Pasqal, bringing an entirely new type of quantum technology to our portfolio. Pasqal is a leading developer of neutral atom-based quantum technology which allows you to manipulate neutral atoms (or atoms with an equal number of electrons and protons) directly so that you can pursue areas ranging from graph-based machine learning and material science simulations to optimization problems and problems governed by differential equations. Neutral atom-based quantum processors operate at room temperature and long coherence times, and have impressive qubit connectivity. Pre-register today for Azure Quantum's private preview of Pasqal.

> "With the coming availability of our system via Azure Quantum and the differentiated range of new digital and analog quantum computational capabilities that it introduces, we hope to accelerate the quantum programs of the platform's community and ultimately help them achieve real-world solutions to the world's most critical challenges."
>
> — Georges-Olivier Reymond, CEO and Founder, Pasqal

With the addition of Pasqal, researchers and developers will be able to enjoy access to neutral atom-based quantum computing from Pasqal; digital, gate-based machines from IonQ, QCI, Quantinuum, and Rigetti; and quantum-inspired optimization (QIO) from Microsoft, Toshiba, and 1Qbit. Not only is Pasqal joining Azure Quantum, but we're also excited to share the latest capabilities available through Azure

Quantum from quantum hardware partners across our ecosystem.

Azure Quantum will be the first cloud platform to enable access to IonQ Aria

IonQ Aria is a new premium system that can run hundreds of accurate quantum gates in a single algorithm, compared to other quantum systems capable of running only dozens of gates at a time. IonQ Aria boasts a record of 20 algorithmic qubits (#AQ)[2], based on measured results using real-world algorithms. In IonQ benchmarking tests, IonQ Aria was able to successfully execute quantum circuits containing more than 550 gates, enabling much larger quantum applications.

> "We've demonstrated that IonQ Aria will allow researchers to execute a multitude of quantum algorithms of practical interest with accuracy and at a premium level of quantum computation. Azure Quantum is the first quantum cloud platform through which we are making IonQ Aria accessible."
>
> — Peter Chapman, President and CEO, IonQ

## Quantinuum's state-of-the-art System Model H1 is available through Azure Quantum

Quantinuum's quantum computers include high-fidelity, fully connected qubits, low error rates, mid-circuit measurement, and qubit reuse. In December 2021, Quantinuum reported its second-generation H1 QPU achieved a measured quantum volume of 2048, an increase of 10 times within one year. In preparation for running on the hardware, developers can refine and debug circuits with the companion Quantinuum emulator with a noise model and scale that mimics the operations of the H1 systems.

## Recently-announced Rigetti Aspen-M-1 will soon join private preview

We've already announced that Rigetti's gate-based superconducting processors would be coming to Azure Quantum and utilizing Quantum Intermediate Representation (QIR) to enable low latency and parallel execution. We're pleased to share that the private preview of Rigetti on Azure Quantum will include access to both Aspen-11 with 40 qubits and the latest Aspen-M-1 with 80 qubits as well as support for the Quil programming language. The Aspen-M-1 is the first multi-chip quantum processor using Rigetti's proprietary modular chip architecture.

> "Along with access to our recently announced Aspen-M-1 system, Rigetti's integration with Azure Quantum also supports the Quil quantum programming language and the ability to program the quantum processor at the pulse level. This low-level access will enable developers to experiment with novel techniques to increase performance, tune to a particular use case, and develop custom gate definitions."
>
> — David Rivas, SVP Systems and Services, Rigetti Computing

[2] #AQ is a metric that IonQ proposed in 2020 to assist in evaluating a quantum computer's utility in real-world settings, with the goal of focusing on practical applicability.

### Quantum Circuits' full-stack system, private preview is coming soon

QCI is building a novel full-stack superconducting circuits quantum computing system with real-time feedback that enables error correction, encoding-agnostic entangling gates. As seen at the 2021 Q2B conference, QCI, the QIR Alliance and Microsoft have successfully collaborated to demonstrate an Azure Quantum implementation of a new random walk phase estimation algorithm that executes on QCI hardware and takes advantage of QCI's capability to execute a quantum program with embedded classical computation. The QCI system will be accessible soon through Azure Quantum's private preview.

### Pre-register today for private previews

Do you want to be one of the first to access these advances in quantum hardware through Azure Quantum? Pre-registration is now open for the private preview of Pasqal and superconducting quantum partners Rigetti and QCI. Let us know if you'd like to participate and join the community of innovators on the Azure Quantum platform.

### Run on real hardware today for free

Have you experienced the thrill of running on real quantum hardware? Whether new to quantum computing or an expert, you can run on quantum hardware available in Azure Quantum for free, with an automatic $500 credit per participating hardware platform or up to $10,000 in credits through the Azure Quantum Research Credits program. Just set up a free Azure account (check out free Azure accounts for students), create an Azure Quantum Workspace in the Azure Portal, and kickstart your quantum journey with Azure Quantum today.

# 18.No Free Lunch Theorem in Quantum Computing

by Shraddha Goled
https://analyticsindiamag.com/no-free-lunch-theorem-in-quantum-computing/

Entanglement, as Albert Einstein referred to as 'spooky action at a distance', refers to a phenomenon by which a particle can 'know' something about another particle even if a huge distance separates them. In quantum entanglement, these two particles are said to be so intertwined that one can infer not only the property of the partner particle but also influence it. When studied by Einstein, he found the phenomenon so baffling it was originally taken as evidence that quantum mechanic models were incomplete.

Quantum computers have components called the qubits, which are linked through entanglement, helping grow their computational power exponentially. This is particularly useful in modern encryption that

is used in banking, and other sectors where securing data is of fundamental importance. Recent studies have shown that quantum computing might also help in boosting machine learning. Another application is simulating quantum systems.

In machine learning, the no-free lunch theorem suggests that all optimisation algorithms perform equally well when their performance is averaged over many problems and training data sets. With the rise of quantum machine learning, it becomes imperative to ask whether there is a quantum analogue of this theorem that would restrict a quantum computer's capability to learn a unitary process with quantum training data.

This was recently studied by a group of researchers who documented their learnings in a paper titled "Reformulation of the No-Free-Lunch Theorem for Entangled Datasets". In their paper, the authors showed that entangled datasets violate the classical no free lunches theorem.

## No-free lunches in quantum learning

The no free lunch theorem entails that a machine learning algorithm's average performance is dependent on the amount of data it has.

"Industry-built quantum computers of modest size are now publicly accessible over the cloud. This raises the intriguing possibility of quantum-assisted machine learning, a paradigm that researchers suspect could be more powerful than traditional machine learning. Various architectures for quantum neural networks (QNNs) have been proposed and implemented. Some important results for quantum learning theory have already been obtained, particularly regarding the trainability and expressibility of QNNs for variational quantum algorithms. However, the scalability of QNNs (to scales that are classically inaccessible) remains an interesting open question," the authors write.

This also suggests a possibility that in order to model a quantum system, the amount of training data might also need to grow exponentially. This threatens to eliminate the edge quantum computing has over edge computing.

The authors have discovered a method to eliminate the potential overhead via a newfound quantum version of the no free lunch theorem. Their study showed that adding more entanglement to quantum computing would lead to exponential scale-up, which was verified using Rigetti's Aspen-4 quantum computer. The researchers suggested an extra set of 'ancilla' qubits with the quantum system that can help the quantum machine learning circuit interact with many quantum states in the training data simultaneously. Study co-author Andrew Sornborger said, "Trading entanglement for training states could give huge advantages for training certain types of quantum systems."

The authors believe that one of the applications of this work is in black box uploading, where we learn a model of quantum experiment and then study it on a quantum computer without requiring to do repeated experiments.

## Challenges with the study

The major issue is the complexity of obtaining the entangled training data; this usually depends on the mode of access to the data. When the user has physical access to the target unitary, it is advantageous to input a state with the reference system so that the user can generate training data with entanglement.

As compared to input with no entanglement, this procedure decreases the average risk more efficiently. Secondly, while the study assumes perfect training, the writers caution that it was possible that exponential scaling may have training difficulty. In the past, several strategies have been proposed to avoid barren plateau (gradients that vanish exponentially in the number of qubits) in quantum neural networks; however, this remains an active area of research.

# 19.How to Prepare for A Cyberattack and Set A Backup Plan

by Kim Komando
https://www.usatoday.com/story/tech/columnist/komando/2022/03/17/how-ready-and-prepared-cyber-attack-threats-increase/7069026001/

In the very first days that the Russia-Ukraine war started, I warned you about 10 Russia-Ukraine cons to expect. We're already seeing evidence of those scams in action. Be sure you're keeping your digital guard up.

Smishing – the insider term for scam texts – is a popular route. Most people are less guarded scanning texts than emails. Look for these signs a text is bad news and how to report it.

Misinformation and misleading posts are slamming social media, too. Here are my tricks to spotting fake Russian accounts and posts.

As sanctions increase and Russia's tactics intensify, it's easy to think that you will not be affected aside from high gas prices. This idea is exactly what will get you into trouble — time to wake up.

## Cyberattacks: What you need to know

In 2020, Russian hackers invaded several federal government agencies, including the nuclear weapons agency. That's small potatoes of what could come. A Russian attack on our fiber optic cables or satellites would take down a ton of critical sectors, like internet traffic, banking, GPS, water treatment facilities, power plants, and the power grid.

Many cybersecurity experts predict large-scale Denial of Service attacks. This attack swamps a website with trillions of pings. The website is so busy answering each ping that it can't respond to anything else. If this happens, government and private industry could take days or even months to sort out.

Wait, there's more. Russia could launch phishing and other attacks to plant dangerous malware and ransomware on business and individual computers and networks.

## What if the internet goes down? Have a plan

Our minds jump to the worst-case scenario in times of distress. Say your internet goes out. Before blaming a large-scale attack, make sure the problem isn't closer to home.

Tap or click here for the best apps you can use to troubleshoot your bad Wi-Fi for Android and iPhone. You can also check outage monitoring site Down Detector if only specific sites aren't loading.

If your internet is out and you have cell service, you can use your phone as a hotspot. You need to set this ahead of time, so you're comfortable using it.

Here's how to turn your iPhone or Android into a mobile hotspot.

.
.
.

# 20.CISA and FBI Warning: Hackers Used These Tricks to Dodge Multi-Factor Authentication and Steal Email from NGO

by Liam Tung
https://www.zdnet.com/article/cisa-and-fbi-warning-hackers-used-these-tricks-to-dodge-multi-factor-authentication-and-steal-email/

Russian state-sponsored hackers have used a clever technique to disable multi-factor authentication (MFA) and exploit a Windows 10 printer spooler flaw to compromise networks and high-value domain accounts. The goal? Accessing the victim's cloud and email.

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) issued an alert about Russian state-sponsored activity that pre-dates recent warnings over cyber activity related to Russia's military invasion of Ukraine.

As early as May 2021, the hackers combined a default configuration issue in a Duo MFA setup at a non-government organization (NGO) with the critical Windows 10 PrintNightmare flaw CVE-2021-34481 to compromise it.

Microsoft patched that elevation of privilege issue in August. Once inside a network, the flaw allowed an attacker to create new accounts on Windows 10 machines.

In the NGO's case, the use of a weak password allowed the attackers to use a password-guessing attack to gain the credentials for initial access. The attackers also used the fact that Duo's default configuration setting allows the enrollment of a new device for dormant accounts.

"Russian state-sponsored cyber actors gained initial access to the victim organization via compromised credentials and enrolling a new device in the organization's Duo MFA. The actors gained the credentials via brute-force password guessing attack, allowing them access to a victim account with a simple, predictable password," CISA said in an alert.

After compromising the account, PrintNightmare came into play, with the attackers using it to escalate privileges to a more powerful admin level and then "effectively" disabled MFA for the compromised account.

"This change prevented the MFA service from contacting its server to validate MFA login – this effectively disabled MFA for active domain accounts because the default policy of Duo for Windows is to "Fail open" if the MFA server is unreachable," CISA explains.

It notes that the "fail open" issue is not specific to Duo.

From there, the operation was repeated but applied to higher-value domain accounts. After disabling MFA, the attackers authenticated to the victim's VPN as non-administrator users and made RDP connections to the Windows domain controllers. They nabbed credentials for additional domain accounts and went on to change the MFA configuration file, allowing them to bypass MFA for these newly compromised accounts.

"Using these compromised accounts without MFA enforced, Russian state-sponsored cyber actors were able to move laterally to the victim's cloud storage and email accounts and access desired content," CISA explains.

CISA outlines several mitigations related to and beyond MFA implementations. The MFA-specific mitigations include:

- Before implementing, organizations should review configuration policies to protect against "fail open" and re-enrollment scenarios.
- Implement time-out and lock-out features in response to repeated failed login attempts.
- Ensure inactive accounts are disabled uniformly across the Active Directory and MFA systems.
- Updating software and prioritizing patching of known exploited vulnerabilities, especially critical and high-level vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
- Require service accounts, admin accounts, and domain admin accounts to have strong, unique passwords.

# 21.Hybrid Quantum Algorithms for Quantum Monte Carlo

by William J. Huggins
https://ai.googleblog.com/2022/03/hybrid-quantum-algorithms-for-quantum.html?m=1

The intersection between the computational difficulty and practical importance of quantum chemistry challenges run on quantum computers has long been a focus for Google Quantum AI. We've experimentally simulated simple models of chemical bonding, high-temperature superconductivity, nanowires, and even exotic phases of matter such as time crystals on our Sycamore quantum processors. We've also developed algorithms suitable for the error-corrected quantum computers we aim to build, including the world's most efficient algorithm for large-scale quantum computations of chemistry (in the usual way of formulating the problem) and a pioneering approach that allows for us to solve the same problem at an extremely high spatial resolution by encoding the position of the electrons differently.

Despite these successes, it is still more effective to use classical algorithms for studying quantum chemistry than the noisy quantum processors we have available today. However, when the laws of quantum mechanics are translated into programs that a classical computer can run, we often find that the amount of time or memory required scales very poorly with the size of the physical system to simulate.

Today, in collaboration with Dr. Joonho Lee and Professor David Reichmann at Colombia, we present the Nature publication "Unbiasing Fermionic Quantum Monte Carlo with a Quantum Computer", where we propose and experimentally validate a new way of combining classical and quantum computation to study chemistry, which can replace a computationally-expensive subroutine in a powerful classical algorithm with a "cheaper", noisy, calculation on a small quantum computer. To evaluate the performance of this hybrid quantum-classical approach, we applied this idea to perform the largest quantum computation of chemistry to date, using 16 qubits to study the forces experienced by two carbon atoms in a diamond crystal. Not only was this experiment four qubits larger than our earlier chemistry calculations on Sycamore, we were also able to use a more comprehensive description of the physics that fully incorporated the interactions between electrons.

## A New Way of Combining Quantum and Classical

Our starting point was to use a family of Monte Carlo techniques (projector Monte Carlo, more on that below) to give us a useful description of the lowest energy state of a quantum mechanical system (like the two carbon atoms in a crystal mentioned above). However, even just storing a good description of a quantum state (the "wavefunction") on a classical computer can be prohibitively expensive, let alone calculating one.

Projector Monte Carlo methods provide a way around this difficulty. Instead of writing down a full description of the state, we design a set of rules for generating a large number of oversimplified de-

scriptions of the state (for example, lists of where each electron might be in space) whose average is a good approximation to the real ground state. The "projector" in projector Monte Carlo refers to how we design these rules — by continuously trying to filter out the incorrect answers using a mathematical process called projection, similar to how a silhouette is a projection of a three-dimensional object onto a two-dimensional surface.

Unfortunately, when it comes to chemistry or materials science, this idea isn't enough to find the ground state on its own. Electrons belong to a class of particles known as fermions, which have a surprising quantum mechanical quirk to their behavior. When two identical fermions swap places, the quantum mechanical wavefunction (the mathematical description that tells us everything there is to know about them) picks up a minus sign. This minus sign gives rise to the famous Pauli exclusion principle (the fact that two fermions cannot occupy the same state). It can also cause projector Monte Carlo calculations to become inefficient or even break down completely. The usual resolution to this fermion sign problem involves tweaking the Monte Carlo algorithm to include some information from an approximation to the ground state. By using an approximation (even a crude one) to the lowest energy state as a guide, it is usually possible to avoid breakdowns and even obtain accurate estimates of the properties of the true ground state.

For the most challenging problems (such as modeling the breaking of chemical bonds), the computational cost of using an accurate enough initial guess on a classical computer can be too steep to afford, which led our collaborator Dr. Joonho Lee to ask if a quantum computer could help. We had already demonstrated in previous experiments that we can use our quantum computer to approximate the ground state of a quantum system. In these earlier experiments we aimed to measure quantities (such as the energy of the state) that are directly linked to physical properties (like the rate of a chemical reaction). In this new hybrid algorithm, we instead needed to make a very different kind of measurement: quantifying how far the states generated by the Monte Carlo algorithm on our classical computer are from those prepared on the quantum computer. Using some recently developed techniques, we were even able to do all of the measurements on the quantum computer before we ran the Monte Carlo algorithm, separating the quantum computer's job from the classical computer's.

This division of labor between the classical and the quantum computer helped us make good use of both resources. Using our Sycamore quantum processor, we prepared a kind of approximation to the ground state that would be difficult to scale up classically. With a few hours of time on the quantum device, we extracted all of the data we needed to run the Monte Carlo algorithm on the classical computer. Even though the data was noisy (like all present-day quantum computations), it had enough signal that it was able to guide the classical computer towards a very accurate reconstruction of the true ground state (shown in the figure below). In fact, we showed that even when we used a low-resolution approximation to the ground state on the quantum computer (just a few qubits encoding the position of the electrons), the classical computer could efficiently solve a much higher resolution version (with more realism about where the electrons can be).

Using our new hybrid quantum algorithm, we performed the largest ever quantum computation of chemistry or materials science. We used sixteen qubits to calculate the energy of two carbon atoms in a diamond crystal. This experiment was four qubits larger than our first chemistry calculations on Sycamore, we obtained more accurate results, and we were able to use a better model of the underlying physics. By guiding a powerful classical Monte Carlo calculation using data from our quantum

computer, we performed these calculations in a way that was naturally robust to noise.

We're optimistic about the promise of this new research direction and excited to tackle the challenge of scaling these kinds of calculations up towards the boundary of what we can do with classical computing, and even to the hard-to-study corners of the universe. We know the road ahead of us is long, but we're excited to have another tool in our growing toolbox.

# 22.Quantum Cryptography: Accelerating Social Implementation Through Successful Experiment with Large-Volume Financial Transaction Data by NICT and Collaborators

https://sj.jst.go.jp/news/202203/n0315-01k.html

TThe group composed of Nomura Holdings (Nomura HD), Nomura Securities, the National Institute of Information and Communications Technology (NICT), Toshiba, and NEC started joint verification on the effectiveness and practicality of quantum cryptography technology in December 2020 and announced on January 14 this year that they succeeded in a verification experiment of highly confidential communication and low-latency transmission of large-capacity financial transaction data via quantum cryptography as a use case for the stock trading business, which strictly requires high-speed, large-capacity and low-latency data transmission; the aim is the social implementation of quantum cryptography technology in the future. With this success, it is expected that the implementation of quantum cryptography technology into fields beyond finance will be accelerated.

The threat of cyber-attacks on financial institutions has increased in recent times, and further strengthening of security measures is required. In stock trading, "algorithmic trading", in which a computer automatically determines the timing and quantity of stock trading orders and repeats orders according to stock prices, quote information, trading volume, etc., is widespread through the industry, and the daily trading volume of in Japanese domestic stock exchanges exceeds 3 trillion yen. This means that a communication method that can withstand a huge amount of transaction data transmission is required.

In this experiment, the group verified, for the first time in Japan, the low latency and resistance to large-volume data transmission when transmitting a large amount of highly confidential data conforming to the message transmission format (FIX format) that is the standard in stock trading. As a result, in this assumed use case, the group was able to confirm the following two points: (1) the throughput is maintained at a level of a conventional system, even if quantum cryptography is applied, and (2) even if a large number of stock orders are placed, highly secure and high-speed quantum crypto-

graphic communication can be realized without depleting cryptographic keys. This joint verification was conducted as part of the Strategic Innovation Promotion Program (SIP) "Photonics and Quantum Technology for Society 5.0 "(Management Office: National Institutes for Quantum and Radiological Science and Technology) led by the Cabinet Office.

In the joint verification system, low latency, and large capacity tolerance were verified using an encryption device that uses a key from quantum key distribution (QKD) equipment that places key information on photons, which are particles of light, and shares encryption keys. For verification, NICT set up a simulated financial transaction environment that imitates investors and securities companies on the test communication network environment "Tokyo QKD Network" built by NICT in 2010. Nomura HD / Nomura Securities developed an application that generates simulated data that matches the messaging data format (FIX protocol), which is the standard for actual stock orders. In addition, two types of encryption methods, One-Time Pad (OTP) and Advanced Encryption Standard (AES), were used to encrypt the transmitted message. Of these, OTP has high security (information-theoretic security) so that no third party with any computing power can decrypt the code. However, since the encryption key required is as large as the transmission data, the problem of the key being exhausted occurs.

Due to these characteristics, this time, AES was used together as a preparation for key depletion. For implementation, the group adopted a high-speed OTP device newly developed by NICT to enable high throughput at the Gbps level. AES, unlike OTP, is not information-theoretic secure but requires astronomical calculations to decrypt and is safe due to its computational complexity (computational security). In this use case, by updating the encryption key generated by QKD in a short time, it was thought that even the AES method has sufficient security strength; subsequently, AES256, which uses a 256-bit key length, was selected as an alternative method for OTP. There are two types of AES256 mounting: a software-based mounting method (SW-AES) and a method using an NEC-developed line encryption device (COMCIPHER-Q), which has lower latency.

Using the above three types of encryption methods: high-speed OTP, SW-AES, and COMCIPHER-Q, the group measured, compared, and verified the communication performance of each. At the time of verification, a test case was set according to the actual stock trading business based on the key exchanged with the high-speed QKD device developed by Toshiba and the QKD device developed by NEC. By measuring the response times of multiple different data encryption methods during large-capacity data transmission, the practicality of QKD and each encryption method was verified.

# 23.Award-Winning Quantum Random Number Generator

by Silke Stähler-Schöpf
https://www.mpq.mpg.de/6704034/03-lela-prize-quantum-random-number-generator?c=2342

The MPQ Photonlab is once again awarded with the LeLa Prize of the Federal Association of German School Labs, this time in the category "experiment of the year".

In the experiment, a laser emits light particles. These hit a beam splitter. There they are either reflected or transmitted. Next to the beam splitter are two detectors that record which event has taken place for each photon. A computer records each individual event as a number 0 or 1. "It is completely up to chance which path each individual photon takes," says Qerimi. The highlight of the experiment is that students can influence the photons by means of a "polarisation rotator", i.e. they can manipulate the binary sequence of the numbers 0 and 1. This means that randomness may not be so random any more. The task now is to find a setting for the "polarisation rotator" in which the randomness is of the highest quality. In this way, the pupils get a feeling for the phenomenon of randomness and quantum physics as a whole.

Pupils can get a further insight into the quantum random number generator with the digital development of the PhotonLab's Flipped Classroom Instruction. There, the students work out the basics independently (from home) and deepen their knowledge by experimenting in the student lab.

# 24.Microsoft Has Demonstrated The Underlying Physics Required to Create A New Kind of Qubit

by Dr. Chetan Nayak
https://www.microsoft.com/en-us/research/blog/microsoft-has-demonstrated-the-underlying-physics-required-to-create-a-new-kind-of-qubit/

Quantum computing promises to help us solve some of humanity's greatest challenges. Yet as an industry, we are still in the early days of discovering what's possible. Today's quantum computers are enabling researchers to do interesting work. However, these researchers often find themselves limited by the inadequate scale of these systems and are eager to do more. Today's quantum computers are based on a variety of qubit types, but none so far have been able to scale to enough qubits to fully realize the promise of quantum.

Microsoft is taking a more challenging, but ultimately more promising approach to scaled quantum computing with topological qubits that are theorized to be inherently more stable than qubits produced with existing methods without sacrificing size or speed. We have discovered that we can produce the topological superconducting phase and its concomitant Majorana zero modes, clearing a significant hurdle toward building a scaled quantum machine. The explanation of our work and methods below shows that the underlying physics behind a topological qubit are sound—the observation of a 30 μeV topological gap is a first in this work, and one that lays groundwork for the potential future of topological quantum computing. While engineering challenges remain, this discovery proves out a fundamental building block for our approach to a scaled quantum computer and puts Microsoft on the path to deliver a quantum machine in Azure that will help solve some of the world's toughest problems.

Microsoft Quantum team reports observation of a 30 μeV topological gap in indium arsenide-aluminum heterostructures

Topological quantum computation is a route to hardware-level fault tolerance, potentially enabling a quantum computing system with high fidelity qubits, fast gate operations, and a single module architecture. The fidelity, speed, and size of a topological qubit is controlled by a characteristic energy called the topological gap. This path is only open if one can reliably produce a topological phase of matter and experimentally verify that the sub-components of a qubit are in a topological phase (and ready for quantum information processing). Doing so is not trivial because topological phases are characterized by the long-ranged entanglement of their ground states, which is not readily accessible to conventional experimental probes.

This difficulty was addressed by the "topological gap protocol" (TGP), which our team set forth a year ago as a criterion for identifying the topological phase with quantum transport measurements. Topological superconducting wires have Majorana zero modes at their ends. There is a real fermionic operator localized at each end of the wire, analogous to the real fermionic wave equation constructed by Ettore Majorana in 1937.

Consequently, there are two quantum states of opposite fermion parity that can only be measured through a phase-coherent probe coupled to both ends. In electrical measurements, the Majorana zero modes cause zero-bias peaks (ZBPs) in the local conductance. However, local Andreev bound states and disorder can also cause zero-bias peaks. Thus, the TGP focuses on ZBPs that are highly stable and, crucially, uses the non-local conductance to detect a bulk phase transition. Such a transition must be present at the boundary between the trivial superconducting phase and the topological phase because these are two distinct phases of matter, as different as water and ice.

We have simulated our devices using models that incorporate the details of the materials stack, geometry, and imperfections. Our simulations have demonstrated that the TGP is a very stringent criterion, rendering it a reliable method for detecting the topological phase in a device. Crucially, the conditions for passing the protocol—the presence of stable ZBPs at both ends of the device over a gapped region with gapless boundary, as established via the non-local conductance—were established before any devices had been measured. Given the subtleties involved in identifying a topological phase, which stem from the absence of a local order parameter, one of the design principles of the TGP was to avoid confirmation bias. In particular, the device is scanned over its entire operating range instead of 'hunting' for a specific desired feature, such as a ZBP.

Microsoft's Station Q, in Santa Barbara, CA, is the birthplace of Microsoft's quantum program. For the last 16 years, it has been the host of a biannual conference on topological phases and quantum computing. After a two-year hiatus of in-person meetings due to the pandemic, the Station Q meetings resumed in early March. At this meeting with leaders in quantum computing from across industry and academia, we reported that we have multiple devices that have passed the TGP.

Our team has measured topological gaps exceeding 30 μeV. This is more than triple the noise level in the experiment and larger than the temperature by a similar factor. This shows that it is a robust feature. This is both a landmark scientific advance and a crucial step on the journey to topological quantum computation, which relies on the fusion and braiding of anyons (the two primitive operations

on topological quasiparticles). The topological gap controls the fault-tolerance that the underlying state of matter affords to these operations. More complex devices enabling these operations require multiple topological wire segments and rely on TGP as part of their initialization procedure. Our success was predicated on very close collaboration between our simulation, growth, fabrication, measurement, and data analysis teams. Every device design was simulated in order to optimize it over 23 different parameters prior to fabrication. This enabled us to determine the device tuning procedure during design.

Our results are backed by exhaustive measurements and rigorous data validation procedures. We obtained the large-scale phase diagram of multiple devices, derived from a combination of local and nonlocal conductances. Our analysis procedure was validated on simulated data in which we attempted to fool the TGP. This enabled us to rule out various null hypotheses with high confidence. Moreover, data analysis was led by a different team than the one who took the data, as part of our checks and balances between different groups within the team. Additionally, an expert council of independent consultants is vetting our results, and the response to date is overwhelmingly positive.

With the underlying physics demonstrated, the next step is a topological qubit. We hypothesize that the topological qubit will have a favorable combination of speed, size, and stability compared to other qubits. We believe ultimately it will power a fully scalable quantum machine in the future, which will in turn enable us to realize the full promise of quantum to solve the most complex and pressing challenges our society faces.

# 25.How Will The Ukraine-Russia Crisis Affect Quantum?

by Matt Swayne
https://thequantuminsider.com/2022/03/10/how-will-the-ukraine-russia-crisis-affect-quantum/

The complexity and vulnerability of quantum devices is nearly matched by the complexity and vulnerability of the quantum ecosystem. As other industries contemplate the effects of war and economic sanctions on their own ability to bring products to market at reasonable prices and times, leaders of quantum companies and research institutions must anticipate the ramifications of this now global crisis.

Like other industries, the most obvious affects will be on supply chains that provide everything from raw materials to highly engineered equipment that make up quantum computers and sensors.

One easy example of this is helium, which is integral to the operation of superconducting quantum computers. Helium sources, earlier stretched thin, was relying on Russian sources, reports Chemical and Engineering News in fall of last year.

They report that Russian state-owned company Gazprom brought 20 million $m^3$ of new helium capacity on-line when it opened three helium production lines at its Amur gas-processing plant in southeast-

ern Russia. A logistics center would also package liquid helium into cryogenic containers to ship around the world.

The facility would increase global supply of helium by about 11% and the hope was that it would lower volatility.

That helium supply, as well as other raw material sourced in Ukraine and Russia and just the general state of the already severely tested global supply chain, are now in jeopardy.

## Jeopardizing a Critical Talent Pool

Russia's ability to produce talent in physics is underscored by the fact that, since the fall of the Soviet Union, five Russians have received Nobel prizes for their work in physics. Russian physicists' work — and the ability for that work to reach the outside world — are now significantly hampered.

Ukrainian universities and their faculty and students are acknowledged as some of the world's best and are a key source of talent for the world's quantum companies and institutions. Here, these Ukrainian centers of learning and their people aren't just a ripple effect in the conflict. They are under direct attack.

In an industry that requires highly specialized scientific and engineering talent, each person is critical to advance both the science and the commercialization of quantum. The loss of talent and the loss of collaboration is almost too difficult to fathom.

## Looming Threat

If the war in the Ukraine has exposed the vulnerabilities of quantum, the crisis has also surfaced its importance. As high-tech weaponry and the critical use of cyber warfare has been on display, military experts now have a preview of what might happen in the hands of an autocratic regime.

Arthur Herman, senior fellow and director of the Quantum Alliance Initiative at Hudson Institute, told The Quantum Insider via e-mail that cyber-security defense should be on everyone's mind now.

"The looming threat of Russian cyber attacks should make every government agency, every bank and financial institution, and every pipeline and power plant think seriously about how to defend themselves from attack, not just now but in the future," said Herman. "Russia's hack into the Colonial Pipeline last year is just a warning shot in a cyber war that could grow very hot if the Ukraine crisis continues to spill over."

He added that, fortunately, solutions to cyber-attacks and quantum computer-derived attacks are being prepared right now and must be taken seriously.

"Fortunately, we have solutions at hand to confront the threat not just now, but the possibility of a future attack by a large-scale quantum computer attack of the kind both Russia and China are racing to develop," Herman said. "These are the quantum-resistant algorithms and quantum-enabled communi-

cation networks that a host of companies in the US, Canada, and Europe are working on and have already deployed."

### Technological Dependence

The conflict is also revealing dependence on less optimal classical technologies, such as current global positioning systems (GPS). For example, satellite-based GPS is often unable to deliver necessary signal strength, remains susceptible to spoofing and lacks certain security features.

"The Ukraine-Russia crisis highlights how dependent we have become on capabilities such as GPS," said Chester Kennedy, President of Research & Security Solutions, ColdQuanta, via email. "We have quickly seen how these capabilities can be degraded or taken offline during a conflict."

He added that the conflict is calling attention to quantum approaches that could be both more accurate and more secure. In fact, ColdQuanta is continuing to make considerable advances in helping cut the ties to satellite-based GPS.

"Fortunately, years of research and development has shown how quantum-based solutions can deliver the same level of — or better — positional awareness that GPS provides today," said Kennedy. "This conflict should jumpstart efforts to strengthen investment in scaling new technologies for operational readiness."

# 26.Encryption Meant to Protect Against Quantum Hackers Is Easily Cracked

by Admin
https://www.scientiststudy.com/2022/03/encryption-meant-to-protect-against.html

One of three cryptography algorithms vying to become a global standard against the looming security threat posed by quantum computers has been cracked in a weekend using a standard laptop. The algorithm is now widely believed to be unfit for purpose.

A range of algorithms for encryption – the process of bundling data up into impenetrable files for safe transmission – are currently verified and approved as secure by the US NIST, and consequently they are used around the world. But these algorithms are set to be made obsolete in coming years by the arrival of quantum computers.

Once developed, these machines promise to vastly exceed the power of classical computers at certain types of problems. One example is quickly finding the prime factors that serve as the multiplicative building blocks of a number – for instance, 3 and 7 are the prime factors of 21. This seemingly innocuous ability will fundamentally break encryption currently used in email, banking and cryptocurrencies.

A total of 69 algorithms believed to be resistant to the increased code-breaking ability of quantum computers were submitted to NIST's Post-Quantum Cryptography competition. These have now been whittled down to four finalists for the task of encryption and three for signing signatures, which are used to verify identity, for example when making a financial transaction.

**Rainbow** is one of the final three signature algorithms. A signature scheme is used to mark a message using a secret key known only to that person. It can then be verified as a legitimate message by a recipient using the sender's public key, which is made available to everyone.

Ward Beullens at IBM Research Zurich in Switzerland was able to take a Rainbow public key and discover the corresponding secret key in just 53 hours using a standard laptop. This weakness would allow an attacker to falsely "prove" they are someone else.

Beullens says that this kind of attack, detailed in a study published by the International Association for Cryptologic Research, makes Rainbow "useless" as a method to verify messages. He had previously developed less serious attacks against Rainbow, to which the creators responded by increasing the complexity of the private and public keys at the expense of efficiency, he says.

"I think my previous attack was also quite serious, and I think it was already obvious that Rainbow was not going to be standardised," says Beullens. "The common feeling among cryptographers seems to be that [the other two finalists in the signature competition] are much more secure."

Current algorithms use public keys, secret keys and signatures that are just a handful of bytes, allowing cryptography to be added onto all sorts of protocols without much additional overhead.

Duncan Jones at Cambridge Quantum says that while all cryptographic algorithms can eventually be broken, there are varying levels of efficiency. Some algorithms require more data to store a public key and secure private key, while others do it using less. Rainbow had already been one of the less efficient algorithms, he says.

"We want to change as little of our cryptography infrastructure as possible. So, things like secure internet connections, they can't easily cope with incredibly large public keys," says Jones. "Rainbow already had larger keys. So in that sense, it was already perhaps not the strongest candidate."

Dustin Moody at NIST told New Scientist that the attack against Rainbow had been verified and that it is now unlikely to be chosen as the final signature algorithm when a decision is made later this month. Unfortunately, it has already seen limited real-world use, including by a cryptocurrency called ABCMint.

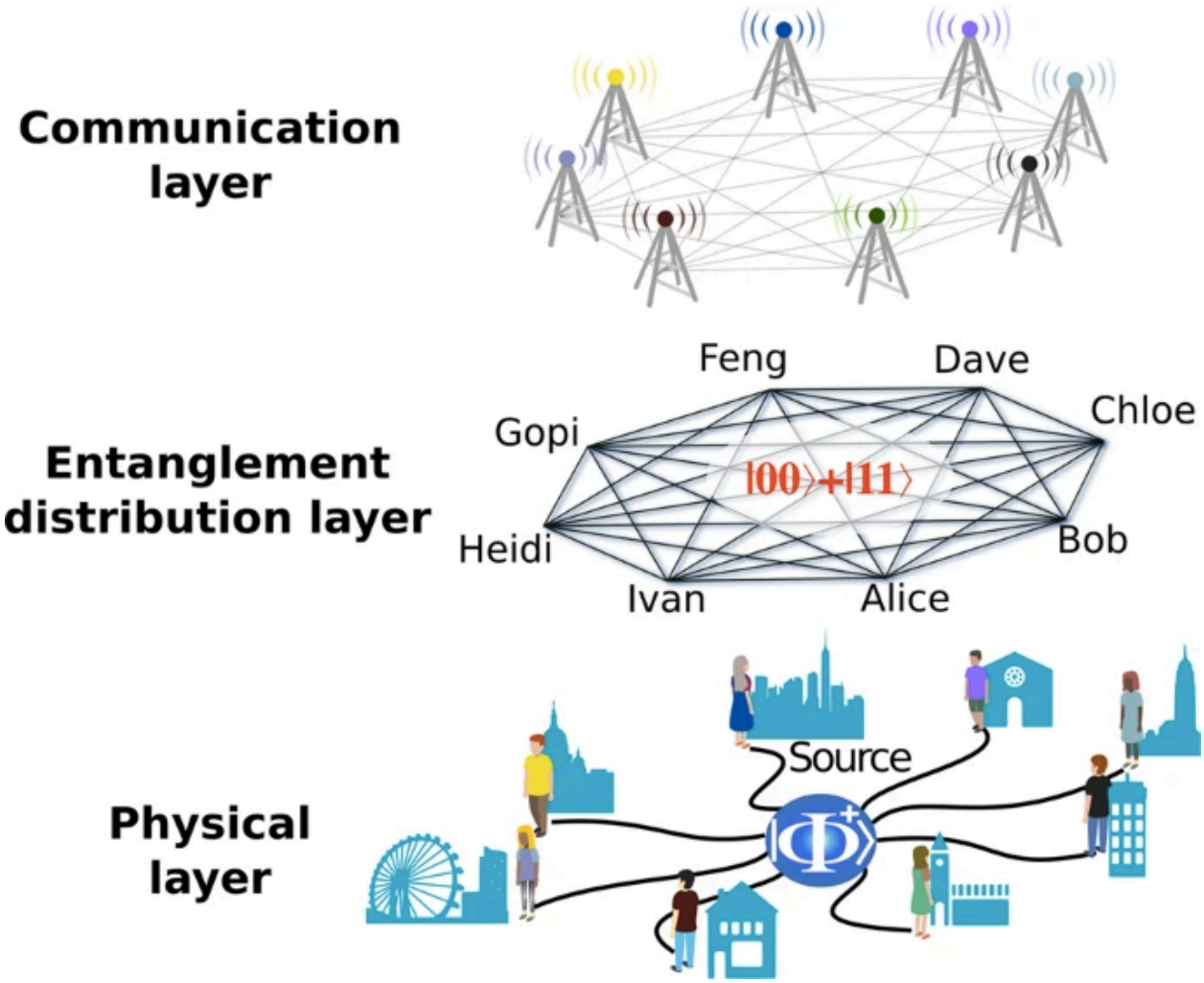
# 27.Experimental Implementation of Secure Anonymous Protocols on An Eight-User Quantum Key Distribution Network

by Karine
https://thequantumhubs.com/experimental-implementation-of-secure-anonymous-protocols-on-an-eight-user-quantum-key-distribution-network/

Researchers experimentally demonstrated five information-theoretically secure anonymity protocols on an eight user city-wide quantum network using polarisation entangled photon pairs.

Anonymity in networked communication is vital for many privacy-preserving tasks. Secure key distribution alone is insufficient for high-security communications.




At the heart of these protocols is anonymous broadcasting, which is a cryptographic primitive that allows one user to reveal one bit of information while keeping their identity anonymous. For a network of $n$ users, the protocols retain anonymity for the sender, given that no more than $n-2$ users are colluding.

This is an implementation of genuine multi-user cryptographic protocols beyond standard QKD.

These anonymous protocols enhance the functionality of any fully-connected Quantum Key Distribution network without trusted nodes.

# 28.Banks Need To Act Now to Ensure Post-Quantum Cybersecurity

by Skip Sanzeri
https://securitytoday.com/articles/2022/03/07/banks-need-to-act-now-to-ensure-postquantum-cybersecurity.aspx?m=1

The Financial Services Industry has long been a lucrative playground for cyber thieves. These days, the push toward a digital banking economy has opened financial institutions to an overwhelming number of new and sophisticated cyberattacks. The list of cyberattacks on banks just in 2021 is long, including Flagstar Bank, the European Banking Authority, New Zealand's central bank, and more. According to a Trend Micro report, banks experienced a 1,318 percent year-on-year increase in ransomware attacks in the first half of 2021.

To make things worse, quantum computers will be used to disrupt service to critical financial cybersystems, which could have devasting effects on the American economy. A study conducted by Arthur Herman at the Hudson Institute revealed that an attack from a quantum computer that disrupts any of the five largest financial institutions' access to the Fedwire Funds Service could cost up to nearly $2 Trillion. It is imperative that banks and financial services institutions take measures to protect themselves and the American economy from these future cyberattacks.

The issue has become so pervasive that during a congressional hearing last year, CEOs from six of the largest U.S. banks testified that cybersecurity is the most significant risk for their industry. The dramatic increase in cyberattacks over the past few years has prompted President Biden, NIST, and the FBI to address growing concerns over our nation's cybersecurity. In addition, in January the White House issued a Memorandum on Improving the Cybersecurity of National Security, which outlines near term standards (including Post-Quantum Cybersecurity (PQC mandates) for National Security Systems (NSS) that are equivalent to or exceed existing cybersecurity requirements.

The challenge of modernizing cybersecurity is exacerbated by the rapid development of quantum computers and the threat of Cryptographically Relevant Quantum Computers (CRQC) which will be capable of breaking public-key encryption.

Public key encryption secures 90% of all global encrypted data. It is used by nearly every U.S. financial institution to secure transactions, client data, online payments, highly valuable information, and IP. Using a quantum algorithm, known as Shor's algorithm, CRQCs will be able to easily factor large prime numbers which form the basis of public-key encryption. Shor's algorithm will be used via a quantum computer to break public-key encryption and access the contents of the encrypted data at financial institutions in the coming years.

In addition to the future CRQC threat directly aimed at financial services organizations, hackers today are harvesting encrypted data with the intention of retroactively decrypting the data using a quantum computer, a process known as "steal now decrypt later." It is rumored that one nation state has already harvested 25 percent of the world's encrypted data, including sensitive information belonging to U.S financial institutions.

It is commonly accepted that the length of time sensitive banking data requires secure protection is at least 25 years. As a result, banks must update their cybersecurity standards now to prevent further loss and liability. Some large financial institutions such as J.P. Morgan, Visa and Barclays are closely monitoring quantum technologies and investing in post-quantum encryption methods to combat classical and quantum attacks. The National Institute of Standards and Technology (NIST) is currently developing standards for post-quantum cryptography, but the implementation of NIST-approved post-quantum algorithms may take decades due to the scale and complexity of today's security networks. NIST is urging enterprises to begin the transition to a new approach called post-quantum cryptography now to protect their data from future attacks.

Post-quantum cryptography (PQC) uses cryptographic systems for classical computers that can protect against quantum computing attacks. Since PQC is software-based, it can be deployed quickly across networks and data. PQC algorithms such as those studied by NIST use complex mathematics such as 400-hundred-dimensional lattice infrastructures to hide a cryptographic key. Studies so far have determined that these chosen algorithms are highly resistant to quantum attacks.

A successful migration to post-quantum cryptography will be judged, in part, by the ease or difficulty of replacing existing systems. Since NIST has not yet finalized its PQC algorithm choices, it is particularly important that financial services organizations remain crypto-agile as part of their overall PQC transition. Crypto-agility means that a bank can start the transition to post-quantum cryptography without making a final choice on NIST approved algorithms. If a financial organization develops the right crypto-agile architecture, it can use any/all of the final NIST approved algorithms. This allows banks to begin testing PQC now, with little or no risk. Financial services organizations can migrate their cybersecurity systems to PQC as NIST continues to finalize post-quantum cryptography standards.

It is also recommended that banks immediately assess their existing systems to determine which components are most vulnerable to quantum attacks and thus need to be prioritized for future updates. Financial institutions can conduct low-cost experiments with hybrid post-quantum and public key solutions, accelerating the transition toward quantum resiliency. Additionally, they can prioritize extremely sensitive data to mitigate risk as the process progresses. Financial institutions must take it upon themselves to conduct these risk analyses now to prepare for the implementation of future NIST post-quantum standards.

To accelerate the transition into the post-quantum era it is critical that financial institutions begin testing practical PQC solutions that minimize disruption to existing systems. These practices and new approaches will play a pivotal role in securing the future of our financial institutions. Banks should look to PQC solutions that offer quantum resilience, crypto-agility and backwards compatibility.

# 29.Stanford Cryptography Researchers Are Building Espresso, A Privacy-Focused Blockchain

by Anita Ramaswamy
https://techcrunch.com/2022/03/07/stanford-crypto-researchers-building-espresso-privacy-scalability-blockchain/

If blockchain technology is to reach true mass adoption, it will have to become cheaper and more efficient. Low transaction throughput on some of the most popular blockchains, most notably Ethereum, has kept gas fees high and hindered scalability. A host of new projects has cropped up to improve efficiency in the blockchain space, each with its own set of tradeoffs, including proof-of-capacity blockchain Subspace, which announced a $32.9 million funding round last week.

Now, a team of researchers from Stanford University's applied cryptography research group has entered the fray. The team is coming out of stealth mode with Espresso, a new layer-one blockchain they are building to allow for higher throughput and lower gas fees while prioritizing user privacy and decentralization. Espresso aims to optimize for both privacy and scalability by leveraging zero-knowledge proofs, a cryptographic tool that allows a party to prove a statement is true without revealing the evidence behind that statement, CEO Ben Fisch told TechCrunch in an interview.

Espresso Systems, the company behind the blockchain project, is led by Fisch, chief operating officer Charles Lu and chief scientist Benedikt Bünz, collaborators at Stanford who have each worked on other high-profile web3 projects, including the anonymity-focused Monero blockchain and BitTorrent co-founder Bram Cohen's Chia. They've teamed up with chief strategy officer Jill Gunter, a former crypto investor at Slow Ventures who is the fourth Espresso Systems co-founder, to take their blockchain and associated products to market.

To achieve greater throughput, Espresso uses ZK-Rollups, a solution based on zero-knowledge proofs that allow transactions to be processed off-chain. ZK-Rollups consolidate multiple transactions into a single, easily verifiable proof, thus reducing the bandwidth and computational load on the consensus protocol. The method has already gained popularity on the Ethereum blockchain through scaling solution providers like StarkWare and zkSync, according to Fisch.

At the core of Espresso's strategy, though, is a focus on privacy and decentralization. The team originally set out a year ago to build a flexible privacy-focused blockchain solution, and has since shifted its priorities to prioritize both privacy and scalability after realizing the "most immediate pain point" for users has actually been the latter, Fisch said.

He added that the broad, industry-wide race to scale blockchain technology has been ongoing since 2018, which is when Solana and other layer-ones first started designing solutions focused on cost-effectiveness and throughput. New projects today face an even more complex challenge, according to

Fisch.

"One thing that's become evident of late is that it's now not just a race to scale, but a race to scale and make the fewest tradeoffs possible with regards to decentralization," Fisch said.

While several different blockchain ecosystems use zero-knowledge proofs to improve efficiency today, that efficiency has come at the cost of decentralization, Fisch said.

"If you use a zero-knowledge proof to prove the validity of a large number of transactions that never get sent to the consensus protocol, then while the consensus protocol can verify their validity, they're not able to provide data to users that is needed for constructing future transactions," Fisch said. Users, then, rely on the ZK-Rollup server for access to that critical data — meaning the data is centralized on that server.

"We're working on a way of integrating the roll-up carefully with consensus so that we still achieve higher throughput and thus lower fees, but without compromising so much on decentralization," Fisch said.

Like decentralization, privacy is another fundamental consideration for many crypto users. Public blockchains such as Ethereum record all transactions anonymously in an electronic ledger open for anyone to view. Although users' identities are encrypted on the blockchain itself, if a particular wallet is linked to an individual, their transactions could be exposed "in real-time to anyone who might care to look, including business competitors and threatening actors looking for targets," according to Espresso Systems.

The company's core privacy solution is a smart contract application called Configurable Asset Privacy for Ethereum (CAPE), which allows asset creators on the blockchain to customize who can see what information regarding the ownership and movement of those assets.

Fisch said that CAPE is particularly well-suited for financial institutions or money service businesses that create blockchain-based assets because it allows them to balance the customer's need for privacy with the institutions' need for risk management and compliance. He shared the example use case of a stablecoin issuer that could create a private version of their coin that allows users to transact privately, while the issuer can still view transaction data.

"CAPE allows asset creators to consider configuring a flexible viewing policy, or even a freezing policy, that gives them more visibility and control over assets that are totally confidential and private to the rest of the public viewing of the blockchain," Fisch said.

CAPE is designed to run on any Ethereum Virtual Machine (EVM) blockchain, and will first debut on the Ethereum testnet in a few weeks so its creators can receive user feedback, though eventually, the application will run directly on the Espresso blockchain, according to Fisch. Espresso is also leveraging Ethereum's popularity as the most widely used blockchain by building a bridge directly to Ethereum that will allow assets to be moved away from Ethereum onto Espresso, according to Fisch.

In addition to its public debut, Espresso Systems also announced today that it raised a $29.9 million

Series A round led by Greylock Partners and Electric Capital, with participation from Sequoia Capital, Blockchain Capital and Slow Ventures. Greylock's Seth Rosenberg, who also backs Chia, led the firm's investment in Espresso Systems.

Espresso Systems raised its seed round in November 2020 led by Polychain, bringing its total funding to $33 million. Its other investors include Alameda Research, Coinbase Ventures, Gemini Frontier Fund, Paxos and Terraform Labs, as well as angel investors Balaji Srinivasan and Meltem Demirors, according to the company.

The team employs 26 people today, 18 of whom are engineers, Gunter told TechCrunch. She added that many of these cryptography-specific engineers joined the Espresso team because of her co-founders' connection to Stanford and the world of academia more broadly (in fact, Fisch was recently hired as a professor of computer science at Yale University).

Gunter said she is confident Espresso can compete against other layer-one solutions working on the same set of issues.

"One advantage that we have is that we have the benefit of getting to design for this and build for this from the outset, whereas a lot of the other systems that are working to scale right now have these big, sort of backward compatibility issues where they're having to design around the existing systems," Gunter said. "If you look historically, other blockchain projects like Solana have had a lot of success being able to start fresh."

# 30.How Artificial Intelligence Is Influencing The Arms Race in Cybersecurity

by Sagar Samtani
https://interestingengineering.com/artificial-intelligence-cybersecurity

The average business receives 10,000 alerts every day from the various software tools it uses to monitor for intruders, malware, and other threats. Cybersecurity staff often find themselves inundated with data they need to sort through to manage their cyber defenses.

The stakes are high. Cyberattacks are increasing and affect thousands of organizations and millions of people in the U.S. alone.

These challenges underscore the need for better ways to stem the tide of cyber-breaches. Artificial intelligence is particularly well suited to finding patterns in huge amounts of data. As a researcher who studies A.I. and cybersecurity, I find that A.I. is emerging as a much-needed tool in the cybersecurity toolkit.

## Helping humans

There are two main ways A.I. is bolstering cybersecurity. First, A.I. can help automate many tasks that a human analyst would often handle manually. These include automatically detecting unknown workstations, servers, code repositories, and other hardware and software on a network. It can also determine how best to allocate security defenses. These are data-intensive tasks, and A.I. has the potential to sift through terabytes of data much more efficiently and effectively than a human could ever do.

Second, A.I. can help detect patterns within large quantities of data that human analysts can't see. For example, A.I. could detect the key linguistic patterns of hackers posting emerging threats on the dark web and alert analysts.

More specifically, A.I.-enabled analytics can help discern the jargon and code words hackers develop to refer to their new tools, techniques, and procedures. One example is using the name Mirai to mean botnet. Hackers developed the term to hide the botnet topic from law enforcement and cyberthreat intelligence professionals.

A.I. has already seen some early successes in cybersecurity. Increasingly, companies such as FireEye, Microsoft, and Google are developing innovative A.I. approaches to detect malware, stymie phishing campaigns and monitor the spread of disinformation. One notable success is Microsoft's Cyber Signals program that uses A.I. to analyze 24 trillion security signals, 40 nation-state groups, and 140 hacker groups to produce cyber threat intelligence for C-level executives.

Federal funding agencies such as the Department of Defense and the National Science Foundation recognize the potential of A.I. for cybersecurity and have invested tens of millions of dollars to develop advanced A.I. tools for extracting insights from data generated from the dark web and open-source software platforms such as GitHub, a global software development code repository where hackers, too, can share code.

## Downsides of A.I.

Despite the significant benefits of A.I. for cybersecurity, cybersecurity professionals have questions and concerns about A.I.'s role. Companies might be thinking about replacing their human analysts with A.I. systems, but might be worried about how much they can trust automated systems. It's also not clear whether and how the well-documented A.I. problems of bias, fairness, transparency, and ethics will emerge in A.I.-based cybersecurity systems.

Also, A.I. is useful not only for cybersecurity professionals trying to turn the tide against cyberattacks but also for malicious hackers. Attackers are using methods like reinforcement learning and generative adversarial networks, which generate new content or software based on limited examples, to produce new types of cyberattacks that can evade cyber defenses.

Researchers and cybersecurity professionals are still learning all the ways malicious hackers are using A.I.

## The road ahead

Looking forward, there is significant room for growth for A.I. in cybersecurity. In particular, the predictions A.I. systems make based on the patterns they identify will help analysts respond to emerging threats. A.I. is an intriguing tool that could help stem the tide of cyberattacks and, with careful cultivation, could become a required tool for the next generation of cybersecurity professionals.

The current pace of innovation in A.I., however, indicates that fully automated cyber battles between A.I. attackers and A.I. defenders are likely years away.

# 31.NIST Set to Announce Round 3 Post-Quantum Cryptography (PQC) Selections Within The Next Few Weeks

https://quantumcomputingreport.com/nist-set-to-announce-round-3-post-quantum-cryptography-pqc-selections-within-the-next-few-weeks/

In December 2016, the U.S. NIST announced a competition to select new quantum resistant public key encryption algorithms that would eventually supersede the classical RSA and other public key cryptography algorithms that may be vulnerable to future quantum computers. For the past five years they have been receiving nominations, holding conferences, and going through three rounds of selection to determine which ones to recommend based upon security, performance, and other factors. They are very close to completing Round 3 and will announce their initial selections of new algorithms to recommend. Some algorithms still need more study and there will be a Round 4 to see if any additional ones should be standardized too. In the chart below, the algorithms shown as Finalists are being considered for standardization in Round 3 and the algorithms shown as Alternates are being considered for further analysis and possible standardization in Round 4.

| | Finalists | Alternates |
|---|---|---|
| KEMs/Encryption | Kyber<br>NTRU<br>SABER<br>Classic McEliece | Bike<br>FrodoKEM<br>HQC<br>NTRUprime<br>SIKE |
| Signatures | Dilithium<br>Falcon<br>Rainbow | GeMSS<br>Picnic<br>SPHINCS+ |

Once the Round 3 selections are announced, NIST will publish a report explaining their decisions. After that, there will still be additional work to draft the standards, call for public comments, and the selections probably won't be officially formalized until 2024. But we see these as activities as formalities that won't create any significant changes. In addition, the Round 4 analysis and recommendation activities will take 12-18 months to complete after the Round 4 candidates are announced.

When we listen to presentations from various consultants and quantum computing providers, we often hear the message that enterprises should start investigating quantum computing now or else they will be left behind. But it is our view that it is just as important, if not more, for enterprises to allocate resources and start right now planning how to migrate their entire digital communications infrastructure to use quantum resistant encryption techniques. Although it may take another 10 years or so before a large enough quantum computer is available to run Shor's algorithm and break the current public key algorithms, experience has shown that it takes 10 years or more to implement new encryption technology in the thousands of computers and software programs that are in use within a typical enterprise.

For those CIOs who experienced the intensive Y2K conversion activities twenty years ago, this migration will likely be significantly more complex. The number of computers, smartphones, IoT, and other digital devices in use today is orders of magnitude higher than it was earlier this century. Also, while Y2K had a specific deadline of December 31, 1999, no one really knows when the large, powerful quantum machines will be in operation. In addition, any communications of long shelf-life data may be vulnerable to a Harvest Now, Decrypt Later attack that accelerates the time frame when quantum resistant encryption is needed. So, enterprises planning a strategy have some important questions to answer such as:

- What systems will we need to upgrade?
- Will PQC support automatically be built into new software updates of programs and apps we are currently using?
- What help can we get from our existing vendors and what new vendors should we bring on to help us?
- Should we use the software-based PQC approach or the physics-based QKD approach?
- Should we look into using hybrid classical/quantum encryption techniques for extra safety?
- Will implementing the PQC algorithms create any performance impacts in our systems and user response times?

With the pending announcement of the first selected algorithms from NIST, now would be the time to get going if you haven't started already. For additional information on this topic, we recommend reading a white paper from the Quantum Economic Development Consortium (QED-C) titled A Guide to a Quantum-Safe Organization. You can also visit the Post-Quantum Cryptography website maintained by NIST which contains an archive of the submissions, presentations, workshops and events that have occurred during this program.

# 32.Thousands Without Internet After Massive "Cyberattack" in Europe

by Agence France-Presse
https://www.ndtv.com/world-news/thousands-without-internet-after-europes-massive-cyberattack-report-2804722?utm_source=newsshowcase&utm_medium=discover&utm_campaign=CCwqGAgwKhAIACo-

HCAowj8n_CjDIrfkCMK7sPTDw8UU&utm_content=bullets

Thousands of internet users across Europe have been thrown offline after what sources said Friday was a likely cyberattack at the beginning of Russia's offensive in Ukraine.

According to Orange, nearly 9,000 subscribers of a satellite internet service provided by its subsidiary Nordnet in France are without internet following a "cyber event" on February 24 at Viasat, a US satellite operator of which it is a client.

Eutelsat, the parent company of the bigblu satellite internet service, also confirmed to AFP on Friday that around one-third of bigblu's 40,000 subscribers in Europe, in Germany, France, Hungary, Greece, Italy and Poland, were affected by the outage on Viasat.

In the US, Viasat said on Wednesday that a "cyber event" had caused a "partial network outage" for customers "in Ukraine and elsewhere" in Europe who rely on its KA-SAT satellite.

Viasat gave no further details, saying only that "police and state partners" had been notified and were assisting with investigations.

General Michel Friedling, head of France's Space Command, said there had been a cyberattack.

"For several days, shortly after the start of operations, we have had a satellite network that covers Europe and Ukraine in particular, which was the victim of a cyberattack, with tens of thousands of terminals that were rendered inoperative immediately after the attack," he said, adding that he was talking about a civilian network -- Viasat.

The outages also knocked offline some 5,800 wind turbines in Germany and Central Europe with a combined output of 11 gigawatts.

"Due to a massive disruption of the satellite connection in Europe, remote monitoring and control of thousands of wind power converters is currently only possible to a limited extent," said the manufacturer, Germany's Enercon which said the problems started on February 24, the first day of the invasion of Ukraine.

"There is no danger to the wind turbines" which continue to produce energy but can no longer be reset remotely if needed, the manufacturer said.

A report by Germany's Federal Office for Information Security said that it was "conceivable that the outages were the consequence of a "cyberattack", German daily Handelsblatt reported.

Military and cyber specialists fear that the Russian-Ukrainian conflict could lead to an outbreak of cyberattacks, a "cyber Armageddon" with major consequences for civilians in Ukraine and Russia, but also globally, through a spillover effect.

But a worst-case scenario has so far been avoided, as the attacks observed appear to be contained in their impact and geographical scope.

Cybersecurity companies have observed attacks in Ukraine that deploy a new data-destroying virus, the actual effects of which are not yet known.

In Russia, institutional websites were made inaccessible from abroad, to protect them from denial of service (DOS) attacks that regularly rendered them inoperable.

# 33.Passwords Aren't Enough - Rethinking IoT Access with Public Key Cryptography

by Carsten Gregersen
https://www.iotforall.com/passwords-arent-enough-its-time-to-rethink-iot-access

Strong security is business-critical in the Internet of Things (IoT) as devices increasingly enter our cars, transporters, aircraft and satellites. Unfortunately, high hacker activity and low device cybersecurity present ongoing causes for concern. Many devices today come with default and publicly disclosed passwords, while others lack even the most basic security. With 27 billion devices expected to be online by 2025, the industry requires trust more than ever. It's for this reason that passwords are no longer enough. It's time for the industry to embrace stronger encryption standards, like public key cryptography.

This status quo is true for even some of our most important devices. For example, a report released in January found that more than half (53%) of internet-connected medical devices contained a known vulnerability, while one-third of bedside devices were identified to have a critical risk. The report warns that if these medical devices were to be accessed by hackers, it would impact service availability, data confidentiality, and even patient safety.

.
.
.

## The Case for Improved Encryption in IoT

One of the best features of this method is that the same public key can be shared with multiple devices or users without security concerns. As a result, the exchange of shared secrets (passwords) becomes unnecessary, and only public keys that are meant to be shared will be shared.

Much more than standalone passwords, public-key cryptography ensures core device security, personal privacy, and adherence to standards and critical maintenance.

As we enter a new era of IoT expansion and integration, these are benefits that must be seriously considered. Ensuring that IoT solutions and projects meet key trust elements is not only important for today's threat landscape, but also for product and service lifecycle challenges that would otherwise inhibit future success. Public key cryptography is uniquely positioned to deliver on the necessary and critical security needs of IoT going forward.

### The Potential of Public Key Cryptography: from Healthcare to Smart Homes

Stronger cybersecurity checks and balances are necessary if we are to depend on devices for increasingly important functions. Hacks have real consequences and, in healthcare, this is especially critical during the pandemic.

In December, The Department of Health in Maryland experienced a ransomware attack that reverberated for weeks. The attack left the department scrambling since it could not release COVID-19 case rates amid the Omicron surge, and the number of COVID-19 deaths was not reported in the state for almost all of December.

Healthcare has become the number one target for cybercriminals in recent years, primarily due to outdated systems and not enough cybersecurity protocols. For example, more than 93% of healthcare organizations experienced some type of data breach between 2016-2019. Solutions like public-key cryptography will go a long way to stopping would-be healthcare hackers in their tracks.

And this is just one sector. As mentioned, connected devices are only growing across our society – from space exploration to smart homes – and users deserve confidence in their products. In this way, the industry must look to stronger protections and improved manufacturer standards, and the widespread adoption of strong, standards-based encryption holds the key.

### Prioritizing Security

Highly regarded in internet security, public-key cryptography meets the specifications to accommodate the requirements of diverse IoT deployments. Therefore, this method is the best option for solution providers to secure data and connected devices in the all-important years to come.

For now, it is incumbent on users to implement strong security protocols with connected devices. Passwords alone are not enough to protect cheap products and users would be foolish to think otherwise. Instead, they are best to incorporate additional security layers and public cryptographic algorithms to bolster their security standing.

# 34.Silkworm Encryption

by Steven J. Vaughan-Nichols
https://thenewstack.io/silkworm-encryption/

Building a bullet-proof encryption system isn't easy. A major component of all classic cryptographic systems is random numbers. But how random is random? All too often random-number generators are fatally flawed. Some run out of entropy, such as billions — that wasn't a typo — billions of insecure Internet of Things (IoT) devices. Others, such as 2008's infamous Debian Linux OpenSSL failure, owe their origin to really sloppy programming. And let's not forget that the NSA used to routinely weaken commercial cryptography by playing random number games. So, why not improve your encryption with

random number generators based on silkworms?

## Silkworms? Silkworms!!? Yes, Silkworms.

Here's how it works. Researchers at South Korea's Gwangju Institute of Science and Technology (GIST) took natural silk fibers from domesticated silkworms. They used this silk to build "sustainable and environmentally-friendly security solutions." They claim that it's "practically unbreachable."

Well, silk is very tough, albeit even spider silk isn't as strong as steel, but unbreachable?

Here's why they say this. This first natural "physical unclonable function (PUF) for environmentally friendly digital security takes advantage of the diffraction of light through natural microholes in native silk to create a secure and unique digital key."

The silk from Bombyx Mori, aka the domesticated silkworm, is filled with microscopic irregularities. Your silk scarf may feel as smooth as fabric can ever be, but its raw form is far rougher.

To generate random numbers from it, Professor Young Min Song, senior author of the study, explained, "When a beam of light hits the disordered silk fibers of an optimal density, it causes light diffraction. The nanostructures in individual microfibers enhance the contrast of light intensity with respect to the background. The diffracted light is then captured by an image sensor. Since the pattern of the microholes is naturally-made, it is unique, giving rise to a unique pattern of light."

## Unbreachable

This is done with a device using a light-reflecting mirror and three tricolor light-emitting diodes The captured light patterns are then converted into a digital format. The researchers claim that "The results were astounding: the average time required to 'fake' the authentication was approximately $5 \times 10^{41}$ years, thus making the LOP-PUF module a practically unbreachable device."

Anytime I hear "unbreachable," my first thought is "You hope," followed by "For now." But that said, this sounds effective. In addition, the equipment needed to generate random numbers from silk is low-cost, portable, eco-friendly, and doesn't require pre- or post-processing. In other words, this could be an inexpensive, reliable way to generate true random numbers for encrypting your messages.

And it's probably cheaper than keeping a wall of lava lamps. "Lava lamps!" you ask? Yes, Lava lamps.

Cloudflare uses lava lamps, aka LavaRand, to generate random numbers for its encryption. Cloudflare's not the only one that use what may at first sound like crazy ways to come up with random numbers. For example, Random.org uses radios that detect lightning strikes around the world for its randomness source. So, while silkworms are certainly... different, they're far from the only odd methods used to create truly random numbers.

# 35.QuiX Quantum Launches New Quantum

# Photonic Processor

by Jonathan Greig
https://kennispark.nl/en/quix-quantum-launches-new-quantum-photonic-processor/

The processor, which was developed at QuiX' facility in Enschede, the Netherlands, outperforms the current generation of processors by almost a factor of 2. The new quantum photonic processor has a record number of qumodes (20), and the highest operating specifications on the market. With this new product, QuiX Quantum continues to push the envelope of photonic quantum computing.

## What Is Quantum Computing?

Quantum computing will revolutionize the way we process information, in fields such as machine learning, chemistry and finance, because of its ability to outperform supercomputers at certain computational tasks.

A quantum photonic processor is a device that can be used to manipulate light for computations. Such processors are the heart of a photonic quantum computer – a quantum computer that uses particles of light as the basic information-carrying units.

## What Makes Quix' Processor Special?

There are two things that matter for a photonic processor – quantity and quality. **Quantity** here means the number of qumodes that the processor can support. Qumodes are the optical equivalent of qubits, the basic information carrying units in the computer – this number should be as high as possible. The **quality** of the processor is set by the amount of light which is lost when traversing over the processor – the less the better. QuiX Quantum has succeeded in producing a processor which has simultaneously very low optical losses and the largest number of qumodes.

With this product launch, QuiX Quantum solidifies its position as the global market leader in photonic quantum computing hardware. QuiX' products distinguish themselves from the competition not just due to their excellent specifications, but also due to their commercial maturity: the system is plug-and-play, and compatible with a large number of other pieces of quantum photonic hardware including all photon sources and detectors currently on the market. For these reasons, QuiX' products have become the de-facto standard for photonic quantum computing across Europe, including the French, German, British, and Hungarian quantum ecosystems.

# 36.Top Government's Budget for Quantum Computing in 2022

by Analytics Insight

https://www.analyticsinsight.net/top-governments-budget-for-quantum-computing-in-2022/

Quantum computing tends to be one of the major disruptive technologies in the nearby future with a promise to simulate complex interactions of atomic structures through smart quantum computers. It also helps in performing fast searches of different kinds of data to solve unapproachable problems efficiently. The governments have started allocating million dollars budgets for investing in quantum computing for 2021-2025. Let's know which country is pacing forward to be at the top of Quantum computing.

**China:** The Government of China announced the funding of a multibillion-dollar quantum computing mega-project with the goal of making important quantum discoveries by 2030. It also pledged billions of dollars to fund the establishment of a Chinese National Laboratory for Quantum Information Sciences.

**The United States of America:** The US Government signed H.R. 6227, the National Quantum Initiative Act, into law in December 2018. (NQI). The law allows a five-year investment of US$1.2 billion in quantum information research.

**France:** The French government has announced a five-year €1.8 billion strategy to boost research in quantum technologies, particularly quantum computers, bringing public funding in the field from €60 million to €200 million per year, putting France in third place behind China and the United States in terms of quantum funding.

**Japan:** For the fiscal year beginning April 2020, Japan's government allotted around 30 billion yen (US$276 million) for quantum research, doubling the previous year's proposal. The technology would also be a focus of a government-funded "moonshot" R&D initiative worth a total of 100 billion yen.

**South Korea:** The new quantum computing research in South Korea will involve a five-year investment of KRW 44.5 billion (US$39.7 million) to create core quantum computing technologies and extend the research base. KRW 13.4 billion (US$11.9 million) has been invested in next-generation ICT technologies, such as ultra-high-performance computing, knowledge data convergence, system software, software engineering, information and intelligence systems, and human-computer interaction (HCI). By 2023, the government hopes to have completed a demonstration of a realistic five-qubit quantum computer system with over 90% dependability thanks to the development of essential quantum computing technologies.

**India:** The Indian Government allocated Rs. 8000 crores for Quantum computing in the 2020 Financial Budget.

**Germany:** In the next four years, the Germany Government will spend around 2 billion euros (US$2.4 billion) to assist the development of its first quantum computer and related technology. Germany's Science Ministry will spend 1.1 billion euros by 2025 to fund Quantum computing research and development, which harnesses quantum physics to provide a leap forward in processing.

That being said, these countries are competing against each other in the Artificial Intelligence race as

well as Quantum computing. Indeed, the future is super-smart for us!

# 37.Researchers Show They Can Steal Data During Homomorphic Encryption

by Matt Shipman
https://news.ncsu.edu/2022/03/stealing-homomorphic-encryption-data/

Homomorphic encryption is considered a next generation data security technology, but researchers have identified a vulnerability that allows them to steal data even as it is being encrypted.

"We weren't able to crack homomorphic encryption using mathematical tools," says Aydin Aysu, senior author of a paper on the work and an assistant professor of computer engineering at North Carolina State University. "Instead, we used side-channel attacks. Basically, by monitoring power consumption in a device that is encoding data for homomorphic encryption, we are able to read the data as it is being encrypted. This demonstrates that even next generation encryption technologies need protection against side-channel attacks."

Homomorphic encryption is a way of encrypting data so that third parties cannot read it. However, homomorphic encryption still allows third parties and third-party technologies to conduct operations using the data. For example, a user could use homomorphic encryption to upload sensitive data to a cloud computing system in order to perform analyses of the data. Programs in the cloud could perform the analyses and send the resulting information back to the user, but those programs would never actually be able to read the sensitive data.

"Homomorphic encryption is appealing because it preserves data privacy, but allows users to make use of the data," Aysu says. "While it has been theoretically possible for a while, homomorphic encryption requires a tremendous amount of computing power. As a result, we are still in the early stages of producing hardware and software to make homomorphic encryption practical."

Microsoft has been a leader in homomorphic encryption, and created the SEAL Homomorphic Encryption Library to facilitate research and development on homomorphic encryption by the broader research community.

"What we've found is that there is a way to 'crack' homomorphic encryption that is done using that library via a side-channel attack," Aysu says. "We were able to do this with a single power measurement."

The researchers were able to verify the vulnerability in the SEAL Homomorphic Encryption Library up through at least version 3.6.

"The library is constantly being updated, so we're not sure if this vulnerability will be addressed in the most recent versions – or if there may be new vulnerabilities that we haven't identified in more

recent versions," Aysu says.

Side-channel attacks are well understood, and there are already countermeasures that organizations can put into place to thwart them.

"As homomorphic encryption moves forward, we need to ensure that we are also incorporating tools and techniques to protect against side-channel attacks," Aysu says.

The paper, "RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library," will be presented March 23 at the virtual DATE22 conference.

# 38.NATO Cybersecurity Center Finishes Tests of Quantum-Proof Network

by Jonathan Greig
https://www.zdnet.com/article/nato-cybersecurity-center-finishes-tests-of-quantum-proof-network/

The NATO Cyber Security Centre (NCSC) has completed its test run of secure communication flows that could withstand attackers using quantum computing.

Konrad Wrona, principal scientist at the NCSC, told ZDNet that it is becoming increasingly important to create protection schemes against current and future threats.

"Securing NATO's communications for the quantum era is paramount to our ability to operate effectively without fear of interception," Wrona said.

"The trial started in March 2021. The trial was completed in early 2022. Quantum computing is becoming more and more affordable, scalable and practical. The threat of `harvest now, decrypt later' is one all organizations, including NATO, are preparing to respond to."

The NCSC, which is run by the NATO Communications and Information Agency (NCI Agency), protects NATO networks around the clock and works with UK company Post-Quantum to conduct the test. Allied Command Transformation's VISTA framework financed the project.

Post-Quantum provides organizations with different algorithms to ensure security even if attackers are using quantum computing. A VPN can use algorithms to secure communications, ensuring that only the correct recipient can read the data, the company claimed.

Wrona said the NCSC does not have a follow-on contract with Post-Quantum but sees the potential of technologies like what Post-Quantum offers and will continue to look into the technology.

Andersen Cheng, CEO of Post-Quantum, called Post-Quantum a 'Hybrid Post-Quantum VPN' because it combines both new post-quantum and traditional encryption algorithms. Cheng said that because it

will take many years for the world to completely migrate to a "quantum-safe" future, it is more realistic to combine these new algorithms with better understood traditional encryption in order to ensure interoperability.

They noted that this kind of software is increasingly relied upon to protect remote connections when working from outside of traditional office environments and can be used to ensure secure communications between organizations in an operational environment.

Cheng founded Post-Quantum 12 years ago and said his team had spent a decade developing encryption capable of withstanding a quantum attack.

His team has focused on building useable commercial grade 'quantum-safe' products like the Hybrid VPN system NATO tested.

"Our encryption algorithm **NTS-KEM** (now known as Classic McEliece, after merging with the submission from renowned cryptographer Professor Daniel Bernstein and his team), is now the only `code-based' finalist in the NIST process to identify a cryptographic standard to replace RSA and Elliptic Curve, for public-key cryptography (PKC). We've also designed a new specification for a quantum-safe VPN as part of the Internet Engineering Taskforce (IETF)," Cheng said.

"We have undertaken work for a number of high-security stakeholders, such as NATO, but the challenges posed by quantum computers are universal. Everything that we do over the internet today -- from buying things online to online banking to nation-state communications -- is encrypted. Once a functioning quantum computer arrives, that encryption can be broken. This means that, almost instantly, bank accounts will be emptied, Bitcoin wallets will be drained, and entire power grids will be shut off."

# 39.A Quantum Solution to an 18th-Century Puzzle

by Karine
https://thequantumhubs.com/a-quantum-solution-to-an-18th-century-puzzle/

A sudoku-style mathematical puzzle that is known to have no classical solution has been found to be soluble if the objects being arrayed in a square grid show quantum behavior. The problem, posed by Swiss mathematician Leonard Euler in 1779, involves finding a way to arrange objects in a grid so that their properties don't repeat in any row or column. The quantum solution might be useful for problems in quantum information processing, such as creating algorithms for correcting errors in quantum computing.

Euler imagined a group of 36 army officers, six from each of six regiments, with each officer having one of six different ranks. Can they be arranged in a square formation such that no regiment or rank is repeated in any row or column?

Solutions can be found for all squares ($3 \times 3$, $4 \times 4$, and so on, assuming the appropriate number of officers) except for $2 \times 2$ and Euler's case of $6 \times 6$. In 1900, the impossibility of a $6 \times 6$ solution was proven by the French mathematician Gaston Tarry. But Suhail Rather of the Indian Institute of Technology Madras (IITM), Adam Burchardt of Jagiellonian University in Poland, and their colleagues wondered if the problem could be solved if the objects were quantum mechanical instead of classical. Then the objects could be placed in combinations (superpositions) of the various possible states: a single officer could be, say, partially a colonel from the red regiment and partially a lieutenant from the blue regiment.

This quantum version requires an adjusted definition of when two such states can be considered "different." Quantum superpositions can be represented as vectors in the space of possible states of the components, and the team assumed that two superpositions are mutually exclusive if their vectors are perpendicular (orthogonal) to one another.

The researchers used a computer algorithm to search for such quantum solutions of Euler's "36 officers" problem. They started from a classical configuration that had only a few repetitions in the rows and columns and tried to improve it by adding in superposition. They found that a full quantum solution to the $6 \times 6$ problem exists for a particular set of superposition states.

A superposition between two quantum objects often implies that they are entangled: their properties are interdependent and correlated. If, say, one quantum officer is found (on inspection) to be a colonel, the other with which it is entangled might have to be a lieutenant. The quantum solution requires a complicated set of entanglements between officers, reminiscent of the entanglements created between quantum bits (qubits) in quantum computing.

The researchers realized that their solution is closely related to a problem in quantum information processing involving "absolutely maximally entangled" (AME) states, in which the correlation between any pair of entangled qubits in the group is as strong as it can possibly be. Such states are relevant to quantum error correction, where errors in a quantum computation must be identified and corrected without actually reading out the states of the qubits.

# 40.100 Million Samsung Phones Affected by Encryption Weakness

by Brandon Vigliarolo
https://www.techrepublic.com/article/100-million-samsung-phones-affected-by-encryption-weakness/

Attention, Samsung Galaxy smartphone owners: There's a good chance your device is one of the 100 million that a Tel Aviv University research paper said suffer from a serious encryption flaw.

Though Samsung patched the vulnerabilities (yes, there's more than one) when the researchers re-

ported it in early 2021, they argue that it's not just about exposing the flaws in a single company's designs; "it raises the much more general requirement for open and proven standards for critical cryptographic and security designs," the paper said.

The researchers didn't stumble upon this error, either: They purposely targeted Samsung devices as an attempt to prove that proprietary, and often undocumented, encryption applications endanger everyone using a smartphone.

## How Samsung breaks its own encryption

Understanding what Samsung has done wrong in its implementation of Android's cryptographic security requires understanding a bit of how the Android operating system is designed. This gets complicated, and there are a lot of acronyms. Consider yourself warned.

ARM-based Android smartphones, which is pretty much all of them, use a split design that separates the top-level Android OS from the TrustZone, a separate bit of hardware that contains a Trusted Execution Environment (TEE) where an isolated TrustZone Operating System (TZOS) lives and makes use of Trust Applications (TAs) to carry out security-related functions.

In essence, when an Android app needs to do something related to user authentication or anything else related to ensuring device security, Android has to send that request to the TZOS. Here's the catch, and the particular thing that the researchers were trying to point out: "The implementation of the cryptographic functions within the TZOS is left to the device vendors, who create proprietary undocumented designs," the paper said.

Vendors like Samsung connect the user-facing Android side (a.k.a., the normal world) with the secure world of the TEE through a hardware abstraction layer that shares data between the Android and TEE worlds via APIs. In the case of Samsung Galaxy devices in the S8, S9, S10, S20 and S21 families, the hardware abstraction layer is managed using an app called the Keymaster TA.

Keymaster TA has a secure key storage area in the normal world that contains keys stored in blob form, meaning that they are encrypted for storage in the normal world, and are decrypted (and re-encrypted) by the Keymaster TA.
The actual decryption is done using an initialization vector (IV), which is essentially a randomized number that serves as a starting value for the decryption operation. These numbers are supposed to be created in the TEE, randomized and unique so that they're harder to decrypt while being stored in the normal world, but that's not the case with the aforementioned Samsung devices, the report said.

The Register pointed out a clarifying Twitter post from John Hopkins Associate Professor of Computer Science Matthew Green, who said that what the researchers discovered was that Samsung is letting the app-layer code (that's run on the normal side) pick the IV key, which makes it trivial to decrypt them.

The end result of apps being able to pick their own IVs is that an attacker could feed their own IVs into key parameters and force the Keymaster TA to use theirs in place of a random one. This is known as an IV reuse attack, which allows attackers to spoof keys, decrypt supposedly secure information

and otherwise gain illicit access to an affected device.

The newer Samsung devices in the S10, S20 and S21 families were designed to resist IV reuse attacks, but the researchers were able to perform a downgrade attack that made the devices resort to vulnerable forms of IV generation that rendered them just as attackable as earlier models.

Additionally, the researchers found that their discovery could also be used to bypass the FIDO2 web authentication method, a passwordless authentication system for websites, by utilizing the downgrade attack they applied to S10, S20, and S21 devices. In short, the attacker can intercept the key generation request from the website, modify it using an IV reuse attack, and then authenticate to the website with the stolen private key.

### Patches are available … this time

As mentioned above, Samsung released patches to affected devices in August and October 2021, essentially making this a non-issue for owners of affected devices that keep them updated.

As the researchers said, Samsung isn't the problem here. It's simply one company making bad use of non-standardized practices and proprietary code that has become a security black box affecting anyone carrying a smartphone.

Damon Ebanks, VP of marketing at digital identity company Veridium, said that it's good that Samsung has released updates addressing these bugs, but that's no reason to understate the seriousness of the threat the researchers uncovered.

"If successful, malicious actors might gain access to the device's normal world sector and install malware, as well as grant root rights to any programs. In addition, rather than running malware in the Android kernel, the attacker might just run code in the Android user mode," Ebanks said.

# 41.Yoo Young-Sang SKT "Metaverse-AI Semiconductor-Quantum Cryptography Global Advancement"

by Natasha Kumar
https://thetimeshub.in/yoo-young-sang-skt-metaverse-ai-semiconductor-quantum-cryptography-global-advancement

"2022 will be the first year in which SK Telecom's next big tech, which was created with know-how accumulated over three years after 5G commercialization, will enter the global market in earnest," said Yoo Young-sang, president of SK Telecom.

It means to reshape the global ICT market based on quantum cryptography based on IDQ along with metaverse platform '**Ifland**' and self-developed AI semiconductor '**Sapion**'.

On the 28th (local time), President Yoo Young-sang held a meeting for reporters in Barcelona, Spain, where MWC22 started, and revealed the strategies of the three next big techs to advance into the global market.

President Yoo said, "It is the result of innovative DNA that differentiates SK Telecom from any other telecommunication company in the world. I am sure it is," he said.

In fact, it is a field that received high interest from various operators around the world at the MWC held three years after the commercialization of 5G. It is explained that cooperation for global advancement beyond the differentiated technology level is also becoming visible.

First of all, ifland, a metaverse service, decided to enter the global market, starting with 80 countries this year. At MWC, the global version was introduced along with the ifland HMD version.

President Yoo said, "At MWC22, requests for collaboration meetings from telecommunication companies from all over the world flooded, and it has established itself as Korea's representative metaverse service in name and reality. We will open a marketplace to increase user convenience."

In the field of AI semiconductors, Sapion successor models will be released by the end of this year or early next year, and the plan is to leap forward as a top-tier global AI semiconductor company.

President Yoo said, "The global market for AI semiconductors is expected to grow by 44% annually and reach 40 trillion won by 2025. was promoted," he said.

Previously, the three companies jointly invested with SK Square and SK Hynix to establish Sapion in the United States to establish a bridgehead to target the global market.

SK Telecom has set a strategy to grow into a company with accumulated sales of 2 trillion won and corporate value of 10 trillion won by 2027 through the launch of next-generation AI semiconductors and global expansion.