Crypto News

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

January 01, 2024

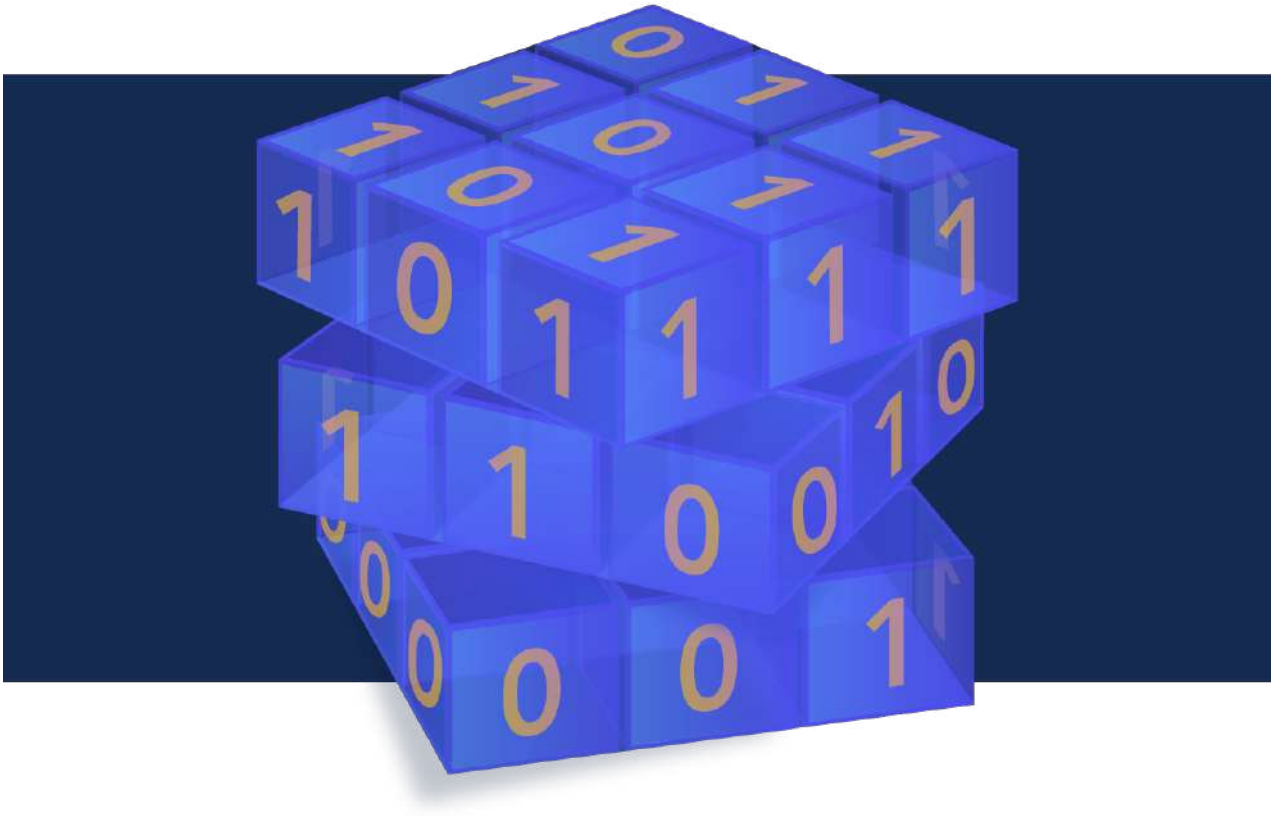


TABLE OF CONTENTS

Editorial

Dear Quantum-Safe Security working group followers,

On behalf of the QSS group, let me wish you all a happy and prosperous new year, with only the best for you and your loved ones. I also hope that 2024 will see some well-needed improvement in the world's affairs. But this is a bit beyond us!

This is our first monthly newsletter of 2024. Since it reports on the last crypto news of 2023, we are clearly in a kind of superposition state. Not surprising in a quantum setting. This actually shows on several of the articles, as a few, such as articles 2, 4 and 14, summarize what happened in 2023 (in cryptography, this is known as an easy problem) while others, such as articles 5, 8, 9, 15 and 26 make the more difficult attempt to forecast 2024 (this is a hard problem).

This superposition makes it an interesting month, with many articles truly worth reading. A personal choice would be:

#8, the Dell story about zero trust and the link between quantum computing and AI, which we will revisit at the QSS this year; #12, which introduces Fully Homomorphic Encryption. To me the ability to keep data in storage encrypted and compute directly without the need for decryption is fascinating. And it could add a lot to security, by focussing the efforts on the security of the datacenter #16 for the Reuters report on the race between the USA and China. And #26, where you see that quantum computing makes it to number 3 in the cybersecurity trends.

Of course, this is highly arbitrary, do feel free to share your thoughts with us.

Have a good reading and again a wonderful year 2024!

The Crypto News editorial is authored by the Chair of the Quantum-Safe Security-Working Group (QSS WG) of the Cloud Security Alliance (CSA), Bruno Huttner, Director of Strategic Quantum Initiatives at ID Quantique SA and it is compiled by Dhananjoy Dey. Both are active members of the CSA 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.

1.Quantum Computing Companies: A Comprehensive 2024 List

by James Dargan
https://thequantuminsider.com/2023/12/29/quantum-computing-companies/

An increasing number of quantum computing companies are emerging globally with the goal of creating operational processors and the hardware and software that enables them. This article looks to provide a high level overview of the landscape of quantum computing companies for now, and into 2024.

Quantum Computing in Less than 200 Words

In sectors like healthcare, cybersecurity and finance, quantum computing (QC) is poised to present novel avenues for tackling computational challenges. In contrast to other intricate tech fields like artificial intelligence (AI) or virtual reality (VR), quantum computing often appears as an enigma to most individuals, save for its practitioners. There exists limited comprehension regarding the potential of a quantum computer or the factors setting it apart from a classical computer.

Harnessing specialized hardware and software, quantum computers are expected to have the capacity to execute tasks which presently lie beyond the reach of conventional computers. Furthermore, quantum computing companies are actively crafting technologies to enhance the accessibility and usability of this state-of-the-art technology.

As fresh innovations continue to emerge, the realm of quantum computing is experiencing rapid expansion. Let's delve into the proliferation of quantum computing enterprises over the past two decades.

The Rise of Quantum Computing Companies

The taxonomy that we have used to classify quantum computing companies has the following sections: "Quantum Computing Giants", "Hardware-focused Quantum Computing Companies" and "Software-focused Quantum Computing Companies", as well as a section for key enablers, which is non-exhaustive. In our review, we include circa one hundred quantum computing companies based on data from our Quantum Intelligence Platform.

It was inevitable that we would have to omit many of the players in the supply chain; our Quantum Intelligence Platform has many more organizations within its database than we could possibly include here. The purpose of this article is to highlight both the leaders in hardware and software quantum computing, as well as the important startups in the industry with promising research, products or services.

Just to give you a heads up, we have also published a few in-depth articles in the past that explore some of the best quantum computing startups, available to read here and here.

The ecosystem of suppliers, hardware companies, and software companies will grow more complex as quantum computing becomes more mainstream. As always, The Quantum Insider will cover them in news stories and include them in our platform. A number of quantum security-related players have also been excluded from this analysis, though some of them have been highlighted when appropriate in both the hardware and software sections.

All the listed companies are in alphabetical order. The list is current as of mid-December 2023.

Top Quantum Computing Companies

- THE CORPORATE GIANTS IN QUANTUM COMPUTING

  Among the prominent entities in the quantum computing (QC) arena originating from the United States – Google, IBM, Microsoft, and AWS (Amazon) – only IBM boasts a legacy of over a century in technological innovation. The remaining trio, comprising Google, Microsoft, and AWS, has a (comparatively) shorter computing history.

  Notably, other significant contenders, which we've encompassed in our consideration, are cognizant of the substantial ramifications that quantum computing and quantum computing enterprises are destined to exert across various domains in the medium and long run. These contenders are initiating their own quantum computing research and development initiatives, driven by the ambition to remain relevant as the industry transcends the era of noisy intermediate-scale quantum (NISQ), advances to fault-tolerant capabilities, and ultimately attains the coveted state of quantum advantage, marking a new era in computation.

  IBM, Google Quantum AI, Microsoft, Amazon Braket, Alibaba Group, Baidu, EVIDEN (Atos Computing), Intel,

- TOP HARDWARE-FOCUSED QUANTUM COMPUTING ORGANIZATIONS

  Alice & Bob, Alpine Quantum Technologies (AQT), Anyon Systems, Atlantic Quantum, Atom Computing, Bleximo, C12 Quantum Electronics, D-Wave, Diraq, EeroQ, Infleqtion (formerly ColdQuanta), IQM, IonQ, Nord Quantique, ORCA Computing, Origin Quantum, Oxford Ionics, Oxford Quantum Circuits (OQC), PASQAL, Photonic Inc. Planqc, PsiQuantum, Quantum Computing Inc (QCI), Qilimanjaro, QuEra Computing, Quandela, QuantWare, Quantinuum, Quantum Brilliance (QB) , Quantum Circuits (QCI), Quantum Motion, Quantum Source, Rigetti Computing, SEEQC, Silicon Quantum Computing (SQC), TuringQ, Universal Quantum, Xanadu,

- TOP SOFTWARE-FOCUSED QUANTUM TECHNOLOGY COMPANIES

  1QBit, Agnostiq, Aliro Quantum, Algorithmiq, A Star Quantum, BEIT, BosonQ Psi (BQP), Entropica Labs, Horizon Quantum Computing, HQS Quantum Simulations, JiJ, Kvantify, Multiverse Computing, PolarisQb, ProteinQure, QC Ware, Quantastica, Quantum Generative Materials, Qubit Pharmaceuticals, QunaSys, Riverlane, SandboxAQ, Strangeworks, Terra Quantum, Zapata AI,

- OTHER KEY ENABLER QUANTUM TECHNOLOGY COMPANIES

  Classiq, Quantum Machines (QM), QuantrolOx, Q-CTRL

Current QC Trends

While the use of the term "trend" may raise eyebrows, especially among those in the scientific and hard tech sectors, where years, if not decades, are spent developing intellectual property and ideas, the landscape of quantum computing in 2023 is undeniably marked by several notable developments.

Firstly, there is a growing consensus that quantum-based encryption is swiftly becoming an issue that needs addressing. Concerns about the potential for malevolent actors to "hoard data for future decryption" once quantum computing reaches functional maturity have prompted many companies and institutions to explore quantum-resistant security alternatives for data transmission.

Secondly, the emergence of Quantum Computing as a Service (QCaaS) is gaining significant increasing

traction. With the proliferation of cloud computing and accessible platforms like IBM, Microsoft Azure, Google Cloud and AWS Braket, the quantum revolution is clearly in progress, offering quantum computational power to a broader audience. Companies are also exploring how to provide private cloud and hosted services to deal with the strict data privacy requirements for end customers.

Thirdly, governments have shown a significant commitment to advancing quantum research, earmarking over $40 billion for the next ten years. This substantial investment is poised to establish seven new national quantum research centers. These centers will serve as hubs for innovation and development in the rapidly evolving field of quantum technology, reflecting a strong and forward-looking approach to harnessing the potential of quantum science.

Next, we have the topic of physical and logical qubits, highlighted in an excellent Linkedin post by Simone Severini, General Manager of Quantum Technologies at AWS and University College London (UCL). In it, Severini presents the fact performance of a quantum computer depends on the number of logical qubits and their logical clock speed, crucial for implementing error-corrected quantum algorithms. Advancements in quantum computing, he believes, are leading toward the Logical Intermediate-Scale Quantum (LISQ) era, with a focus on balancing fidelity, clock speed, and error correction to enhance quantum computing capabilities.

Lastly, the concept of a quantum internet, designed to facilitate communication by harnessing the enigmatic principles of quantum mechanics, is on the horizon. Although its widespread implementation may still be some time away, experts in the field are openly discussing it, particularly in light of China's notable advancements in this domain.

Quantum Computing Companies Summary

As always, The Quantum Insider team strives to provide a detailed yet non-exhaustive resource. We trust that our list has provided valuable insights into some of the world's most prominent and generously funded quantum enterprises, spanning both hardware and software domains.

If you've found this article enlightening, we invite you to delve deeper into the latest developments in quantum technology by perusing our extensive coverage of current news in the quantum realm. Additionally, for a more in-depth exploration of enterprise end users leveraging quantum technology, we encourage you to explore our dedicated Market Intelligence platform, which offers a thorough examination of this exciting landscape.

2.Quantum Industry's Milestones of 2023: Breakthroughs and Innovations

by Wojciech Zylm
https://bnnbreaking.com/world/russia/quantum-industrys-milestones-of-2023-breakthroughs-and-innovations/

In a year marked by significant scientific progress, the quantum industry has emerged as a distinct trailblazer throughout 2023. A series of notable advancements and breakthroughs have served to propel the field to new heights, firmly establishing quantum technology as an arena of boundless potential and increasing global interest.

Leap into Quantum Computing

Among the most striking milestones was the unveiling of a 16-qubit quantum computer by Russian physicists. This impressive machine, which integrates trapped ion and photonics approaches, signals Russia's inaugural foray into the dynamic field of quantum computing. Simultaneously, a groundbreaking double slit experiment conducted in the time domain by an Imperial College-led research team has extended the classic wave-particle duality to time itself, further deepening our understanding of quantum mechanics.

AI Meets Quantum Science

In a fascinating blend of artificial intelligence and quantum concepts, GPT-4, a state-of-the-art large language model, was subjected to a quantum information science exam by Scott Aaronson. The model achieved a **B grade**, underscoring the potential of AI in grasping and interpreting complex quantum principles.

Collaborations and Innovations

On the industry front, Intel has launched a 12-qubit silicon quantum research chip, intriguingly named **Tunnel Falls**. In a bid to further quantum computing research, the tech giant has also joined forces with the Qubit Collaboratory at the University of Maryland. In a unique cultural twist, a Lego enthusiast has proposed the idea of a quantum computing Lego set, reflecting the pervasive influence of quantum technology in contemporary society.

Investments and Advancements

Governmental entities are also showing a keen interest in the quantum realm. Germany, for instance, has announced a substantial 3 billion euro investment plan aimed at developing a universal quantum computer by 2026. Meanwhile, a team in South Korea has created a room temperature superconducting material, LK-99, which could potentially revolutionize multiple industries, including quantum computing.

Visualizing Quantum Mechanics

A landmark collaborative research effort has achieved the visualization of entangled photons' wave functions in real-time, marking a significant stride in the visualization of quantum mechanics. Adding to the list of accomplishments, Google scientists have claimed a quantum advantage by completing a computational task in a fraction of the time required by classical supercomputers. Meanwhile, QuTech researchers have refined the Andreev spin qubit, which could be pivotal in the quest for the perfect qubit for quantum computers.

As 2023 draws to a close, the advancements in quantum technology not only reflect the industry's rapid progress but also underscore the potential of quantum computing to redefine our understanding of the universe and catalyze transformative changes across multiple sectors.

3.Saving Schrödinger's Cat: Getting serious about post-quantum encryption in 2024

by Sydney J. Freedberg Jr.

https://breakingdefense.com/2023/12/saving-schrodingers-cat-getting-serious-about-post-quantum-encryption-in-2024/

For decades, most digital communication has relied on an algorithm called RSA, invented in 1977 to allow two parties to communicate securely without having to exchange secret codes beforehand. Starting in 2024, that's going to have to change.

Specifically, government agencies and private companies need to begin combing through countless lines of software code to find every instance of RSA and other long-standard protocols, so they can ultimately replace them with Post-Quantum Cryptography (PQC), a new set of algorithms designed to resist rapidly advancing quantum computers which could, in theory, crack any existing encryption.

The issue is urgent for agencies and companies have data that's both highly sensitive and likely to remain relevant for many years, like performance and design specs for military vehicles and weapons systems. That's the kind of encrypted data a well-heeled intelligence agency, like China's Ministry of State Security, might spend the resources to scoop up now, even though they can't decrypt it yet, and then store it until the long-awaited RSA-killing quantum computer arrives — a strategy known as "harvest now, decrypt later."

If someone's already run a "harvest" operation against you, one attendee at a recent ATARC webinar asked, what can you do to protect yourself? Not much, said Bill Newhouse, a senior cybersecurity engineer at the National Institute of Standards & Technology: "Unfortunately, that data's out."

What makes quantum computing such a game-changer? Every digital device in widespread use today — from baby monitors and microwave ovens to smartphones and smart missiles — uses thousands of tiny integrated circuits to store and manipulate information. If the circuit is holding enough electrical charge, it's "on" and counts as a "1" in binary logic; if it's not charged, it's "off" and counts as "0." Every function a digital device can perform boils down to adding and subtracting 1s and 0s over and over and over at superhuman speed.

This works great for a surprising range of applications, from the obviously mathematical, like tax prep software and encrypted messaging, to the seemingly creative, like generative AI making songs and videos. But the 1s and 0s struggle with computations that involve a huge number of different variables, like simulating how a new enzyme might behave or breaking an enemy code.

Quantum computers get around that problem by using "quantum bits," or qubits, which exploit the ambiguous nature of subatomic particles to embody every possible value between 0 and 1. It's a practical application of Schrödinger's Cat, the famous thought experiment where a trapped animal is neither alive nor dead, but both and neither and all states in-between. While "macroscopic" objects such as cats don't actually behave this way, subatomic objects do, which means quantum computers can carry out calculations far too complex for classical computers — which, in time, will probably include including breaking RSA.

Late last month, NIST formally closed the public comment period for three PQC algorithms it plans to finalize for widespread use next year. But NIST finalizing algorithms doesn't solve the problem: That takes everybody implementing them.

"This is huge," said Newhouse. "This migration [to PQC] should be the biggest one ever undertaken," he told the ATARC webinar, at least since software began using RSA and other public key encryption in the first place decades ago.

A crucial caveat: That doesn't mean everyone should leap to install the new algorithms now. In fact, you're not supposed to until they're finalized. Technically, Newhouse said, "you *could* use them, but

you'd be in violation of some rules, [because] you have to have a FIPS [Federal Information Processing Standard] validated product and that's not there yet."

"Those three drafts are just finished receiving comments," he noted at the Dec. 5 webinar. "[NIST] will be adjudicating those comments, making the final publication even better because people submitted things they noticed." And NIST takes outside input seriously: It had originally planned to release four new algorithms until independent testing revealed fatal flaws in one of them just last year.

"These open standards and these validation processes mean you're getting a lot of eyes on this technology before you're equipped with it," Newhouse said at a Defense Scoop event on the same day.

Once NIST finalizes the PQC standards, however, there are yet more steps before anyone can use them. Software companies have to implement the new cryptography algorithms in actual code a computer can run — and that code should go back to NIST for Cryptographic Module Validation to ensure it actually works. That can take "months or years," Newhouse acknowledged.

But that doesn't mean agencies and companies should just sit around waiting for their favorite cybersecurity vendor to come up with a PQC implementation, Newhouse and other experts emphasize. Far from it: Firms should already be taking inventory of the software your organization uses, so you can find where it uses RSA and other soon-to-be-superseded encryption protocols that will have to be replaced with the new PQC algorithms. And because RSA can crop up in all sorts of unexpected places — basically every time one computer wants to communicate something securely with another — it can take a long, long time to find every instance.

"It impacts everything we do, from switches to routers to our most prized possessions, our critical weapons systems," said Wanda Jones-Heath, principal cyber advisor for the Air Force, speaking at the Scoop News event. "If we had not started this two years ago, we would be even further behind."

As hard as hunting out instances of RSA can be for private companies, it's even more complicated for government organizations, both military and civilian, which tend to use a patchwork of technologies of varying ages. "Federal networks are weird," said Nick Polk, senior advisor to the Federal Chief Information Systems Officer in the Executive Officer of the President. "We have legacy IT from the seventies out there still … [and] encryption is everywhere."

Software companies are already offering automated "discovery" tools, designed to inspect code and find instances of encryption that will need to be replaced. But there's still no easy fix, so both finding the problem and fixing it will be the work of years.

With that laborious timeline in mind, a White House National Security Memorandum issued last year gave federal agencies until 2035 to complete their migration to post-quantum encryption. But that deadline assumed it would take many years for today's experimental quantum computers to evolve into "cryptographically relevant" machines able to break RSA, an assumption challenged by a recent breakthrough by a DARPA-funded, Harvard-led research team.

That advance — a quantum leap in quantum computing — could bring the end of RSA and other long-used encryption years closer for everyone.

4.Top Ten Favorite Quantum News Stories of 2023

by Matt Swayne
https://thequantuminsider.com/2023/12/28/top-ten-favorite-quantum-news-stories-of-2023/

We expected an “interesting” year in quantum 12 months ago.

We were right, but not always in ways we expected.

Emerging from a pandemic, facing a sharp economic lull, diving deep into the incredibly baffling world of quantum science and battling against a range of political and military conflicts, the quantum industry felt at times like a roller coaster of good news stories and bad news stories.

Close to 2 million people checked out stories about quantum research advances, funding rounds, and Lego’s quantum computing proposal on The Quantum Insider this year — and here are the top ten Quantum news stories of 2023, according to our own analytics.

#1 RUSSIAN SCIENTISTS PRESENT 16-QUBIT QUANTUM COMPUTER

A team of Russian physicists presented a 16-qubit quantum computer at the Forum for Future Technologies in Russia that appears to combine trapped ion and photonics approaches, according to a post from Rosatom, the Russian State Nuclear Energy Corporation . The computer is the first quantum computer developed in Russia, according to the post, which was translated into English by a computer. The device is still in the early stages of development and is small by standards already achieved by global quantum leaders. However, it has the potential to be a powerful tool for research and development, the scientist said. The team added that they have already used the device for simulating simple molecules.

#2 CHATGPT-4 RECEIVES ‘B’ ON SCOTT AARONSON’S QUANTUM INFORMATION SCIENCE FINAL — IMMEDIATELY EMAILS THE DEAN SEEKING A BETTER GRADE

In a recent experiment, noted quantum expert and educator Scott Aaronson had GPT-4 take the actual 2019 final exam from Introduction to Quantum Information Science, an honors upper-level undergrad course at UT Austin. The resulting grade — a B — did not sit well with the large language mode — LLM — system. According to a blog post on Aaronson’s blog Shtetl-Optimized, Aaronson and his head teacher’s assistant gave GPT-4 the problems via their LaTeX source code. Quantum circuit answers relied on a qcircuit package, which GPT-4 again understands, or used an English description of the circuit.

#3. TIME IS ON MY SIDES: RESEARCHERS SHOW DOUBLE-SLIT EXPERIMENT ALSO APPLIES TO TIME

Scientists have been able to confirm the wave-particle duality of quantum objects like photons, electrons and atoms through double-slit experiments.

Now it looks like it’s time’s turn.

In a study published in Nature, an Imperial College-led team of researchers were able to create a time-domain version of the double-slit experiment using a beam of light that was twice gated in time.

#4 INTEL ANNOUNCES RELEASE OF ‘TUNNEL FALLS,’ 12-QUBIT SILICON CHIP

Intel announced the release of its newest quantum research chip, Tunnel Falls, a 12-qubit silicon chip, and it is making the chip available to the quantum research community. In addition, Intel is collaborating with the Laboratory for Physical Sciences (LPS) at the University of Maryland, College Park’s Qubit Collaboratory (LQC), a national-level Quantum Information Sciences (QIS) Research Center, to advance quantum computing research.

#5 LEGO POISED TO ENTER THE QUANTUM COMPUTER MARKET

Disregarding an ever-increasing number of modalities and approaches and indifferent to the intense competition from savvy startups and techno giants, Lego could enter the race to build a quantum computer.

Well, at least one Lego fan designer is readying the Denmark-based toy company for the quantum era.

In a product suggestion, a Lego user pitched creating IBM Quantum Computer System in Lego Ideas, a site that allows users to submit suggestions for future logo sets.

#6 YIN-YANG? RESEARCHERS CAPTURE THE MYSTERIOUS DANCE OF ENTANGLED PHOTONS IN REAL-TIME

Researchers at the University of Ottawa, in collaboration with Danilo Zia and Fabio Sciarrino from the Sapienza University of Rome, recently demonstrated a novel technique that allows the visualization of the wave function of two entangled photons, the elementary particles that constitute light, in real-time.

#7 GOOGLE CLAIMS LATEST QUANTUM EXPERIMENT WOULD TAKE DECADES ON CLASSICAL COMPUTER

Staking another claim of quantum advantage, Google scientists are reporting that they completed a computational task on a quantum computer that would take a classical supercomputer 47 years to complete, the Telegraph reports. Google scientist published their findings on the pre-press server ArXiv. Scientists often use the server to distribute findings before seeking official peer review.

#8 GERMANY ANNOUNCES 3 BILLION EURO ACTION PLAN FOR A UNIVERSAL QUANTUM COMPUTER

Germany's action plan for quantum technologies is set to invest a total of 3 billion euros in the development of a universal quantum computer by 2026, according to the federal government's "action concept for quantum technologies," according to German media.

The aim is for Germany to catch up with international development in the US and China. Of the 3 billion euros, the lead research ministry will receive 1.37 billion euros of the funds, with an additional 800 million euros in the budgets of state-financed research institutes. The cabinet is expected to launch the concept by the end of April.

#9 HOW WOULD ROOM-TEMPERATURE SUPERCONDUCTORS CHANGE QUANTUM COMPUTING?

With news that a South Korean research team created a superconducting material — LK-99 — that reportedly operates at room temperature and at ambient-pressure, the scientific world — and even the mainstream media — are speculating how this technology could be tapped and what would be the resulting benefits. The inventors of the room-temperature superconducting material — LK-99 — speculate the invention would disrupt nearly every industry on some level and call out quantum specifically.

They write in their paper on the invention: "The LK-99 has many possibilities for various applications such as magnet, motor, cable, levitation train, power cable, qubit for a quantum computer, THz Antennas, etc. We believe that our new development will be a brand-new historical event that opens a new era for humankind." It's important to note that while room-temperature superconducting advances may clear some of the scalability hurdles, warm temperatures still impact quantum errors. That being said, and

while scientists are still trying to verify this work, how will it affect quantum computing? If at all?

#10 DELFT RESEARCHERS SAY THEY FOUND A PRIME CANDIDATE FOR 'THE PERFECT QUBIT'

Researchers from QuTech improved the so-called 'Andreev spin qubit' in a critical way and believe it can become a prime candidate in the pursuit of a perfect qubit. The new type of qubit is created in a more reliable and intrinsically stable way, compared to previous versions, by combining the advantages of two other types of qubits. They publish their work in Nature Physics.

5.Top Predictions in Quantum for 2024

by Matt Swayne
https://thequantuminsider.com/2023/12/27/top-predictions-in-quantum-for-2024/

Making predictions about the quantum industry is not easy.

I would say the accuracy of my last year's list of predictions were a little better than chance — but, still, it's a great opportunity to explore the possibilities and start some conversations. And, fool's errands are kind of my thing.
So, with that, let's take a look at What Might Be in the world of quantum research and development, quantum industrial trends and quantum's impacts on society.

The Dawn of Quantum Practicality

The term, "Quantum Practicality," entered the lexicon in earnest in 2023, probably chosen because it sounds less hubristic than quantum advantage and, certainly, quantum supremacy. Like those terms, quantum practicality is hard to define and, therefore, hard to measure. However, in 2024 we should see of a glimpse of achieving the spirit of that term.

In other words, expect a few companies and research institutions to perform everyday computational tasks using quantum computers with a performance better than classical. Also, expect those results to be challenged. In 2024, the results won't be enough to convince many in the mainstream community that quantum is a viable alternative to supercomputers, let's say, but as the frequency of quantum practicality reports in 2024 increase, a lot of those doubters may be converted.

Quantum Startups Explore Other Commercial Options

The financial pullback probably meant that many quantum startups didn't quite finish building their runway when they taxied onto the tarmac. For many startups, this could be an existential crisis. For other startups, this could be an existential opportunity.

While working on their main products, expect some quantum organizations to explore other ways to raise revenue. Some of these could be quite traditional ways of bringing in income — consulting is probably the most common. However, quantum companies may find ways to nourish current needs on the market, rather for waiting until the full blossoming of the quantum market. Creating products in nuclear medicine, as one example, might be one area that requires quantum-like expertise and skills.

But there are other known-unknown and unknown-unknown markets for smart startups to stumble on to, or even create.

Private Capital Markets Begin to Stabilize

Over the past three years, it's been feast and famine for quantum startups seeking funding in the pandemic-battered, geo-politically charged, interest-rate challenged investment market. In 2023, we saw a dramatic drop in the number — and, arguably, the size — of finding rounds.

In 2021 and 2022, quantum companies brought in record amounts of money for the albeit nascent quantum industry. In late fall 2023, we did see private capital return to the quantum industry, although not enough to make any attempt to return to the levels set in the previous two years. It was enough, however, to give the ecosystem some faith that the market will stabilize. And, that's our expectations, too.

We may not soar to new fund-raising heights, but — barring any geopolitical, health crisis, etc. etc. — patient private capital will write checks this year for promising quantum tech startups. Another wild card from the opposite hand: Research advances — we like to avoid the term, "breakthroughs" — could wildly inflate the market, bringing in investments from more traditional capital sources not normally associated with deep tech investing.

Urge to Merger, a Fire to Acquire

Let's consider several factors in today's quantum investment landscape:

- First, we've seen a drop in funding for quantum startups.
- Second, quantum startups are — forgive the technical terminology — really freaking expensive.
- Third, research results have been promising, which is liable to attract big companies that have sat on the sidelines.

One potential way of connecting these threeish trends is to consider the landscape a tempting area for mergers and acquisitions. Companies without quantum assets instantly gain a path toward quantum, and quantum entrepreneurs get some added runway. Look for more mergers and acquisitions to occur in 2024.

Make No Mistake — Scientists Will Focus on Quantum Error Correction

Error correction sits at an interesting intersection in quantum science today — scientists know it is critical to creating quantum computers that can perform at levels needed to be adopted more broadly and scientists are also discovering quantum error and quantum mitigation approaches that are beginning to pay off.

This nexus of desire and capability will likely turn into quantifiable results and that should lead to bumps in QC performance, as mentioned above. Ultimately, like a virtuous pool shark running the table, this could lead to a chain-reaction of better quantum computers being unleashed on problems and opportunities in ways that classical computers cannot. These better performing machines could encourage developers to improve quantum algorithms to drive further improvements, or tackle new use cases.

Quantum Joins The Deep-Tech Convergence

We will continue to see a convergence of transformational technologies, the most obvious being quantum and artificial intelligence. But, this trend will go beyond the blending of information technologies.

Many scientists investigating the cutting edge of frontier techs — such a genetic therapies, drug design and fusion energy — will realize the potential for quantum computing to hack the seemingly insurmountable problems that lie at the heart of their technologies' ultimate commercialization.

While quantum sensors to take rides to space, quantum algorithms will dive into understanding the human body, probe the design of fusion reactors and guide new approaches to AI.

Talking Quantum

We mentioned there will be a drive for quantum practicality — leveraging quantum technologies for real-world computational challenges. However, soon or later, the quantum industry will face the need to explain that practicality. This will lead to some interesting — and thorny — conversations. Quantum experts and enthusiasts will need to discuss principles, such as entanglement and superposition, with regular folks.

This may lead to a broadening of our understanding of quantum into disciplines not normally associated with science and informations science, such as sociology, psychology, philosophy and religion.

These conversations might start out as awkward and uncomfortable, but could eventually lead to stronger and richer connections between science and those interdisciplinary communities than ever.

Arts and Qrafts

Expect that as quantum technology moves more toward practicality and interdisciplinarity that it will force non-STEM disciplines to grapple with its implications. As mentioned, philosophers, religious thinkers and ethicists will prove the deeper meaning of quantum technology. Artists will follow — and soon lead. We will see people from the arts — from sculptors to painters to musicians — attending quantum events, or creating their own as a way to explore and interpret quantum information science.

We can all this trend “Q-STEAM.”

6.The Impact of Quantum Computing on Cryptocurrency Security

https://macsources.com/the-impact-of-quantum-computing-on-cryptocurrency-security/

Cryptocurrencies, built upon the principles of decentralized blockchain technology, have gained widespread acceptance in recent years. However, as technology advances, so do potential threats to its security. One such emerging threat is quantum computing, a paradigm that leverages the principles of quantum mechanics to perform computations exponentially faster than classical computers. This article delves into the potential ramifications of quantum computing on cryptocurrency security, exploring the vulnerabilities and proactive measures required for a secure digital future. Platforms such as trade 2.0 intal provide a modern approach to Bitcoin’s online trading ecosystem.

Understanding Quantum Computing

To comprehend the impact of quantum computing on cryptocurrency security, it’s crucial to understand the fundamentals of quantum computing. Unlike classical bits, quantum bits (qubits) exist in a state of superposition, allowing them to represent both 0 and 1 simultaneously. This unique property enables quantum computers to perform parallel computations, exponentially increasing their processing power compared to classical counterparts.

Current State of Cryptocurrency Security

Cryptocurrencies rely on cryptographic algorithms to secure transactions and maintain the integrity of the blockchain. Common algorithms include RSA and ECC, which are vulnerable to quantum attacks. The threat lies in Shor's algorithm, capable of efficiently factoring large numbers, compromising the security of widely used encryption methods.

Real-world implications of quantum threats are already surfacing. The security landscape of cryptocurrencies is evolving, necessitating a proactive approach to address potential vulnerabilities.

Quantum Threats to Cryptocurrencies

Shor's Algorithm and Its Impact

Shor's algorithm poses a significant threat to current cryptographic systems. It has the capability to factorize large numbers in polynomial time, breaking widely used algorithms like RSA and ECC. Once a quantum computer implements Shor's algorithm, it could decrypt encrypted information, compromising the security of transactions and user data.

Grover's Algorithm and Hash Functions

Grover's algorithm, while not as immediately threatening as Shor's, has implications for hash functions commonly used in blockchain technology. Grover's algorithm accelerates the process of finding pre-images of hash functions, potentially reducing the security of cryptocurrency networks. As a result, blockchain projects need to consider quantum-resistant cryptographic algorithms to mitigate these threats.

Quantum-Resistant Cryptography

Post-Quantum Cryptography

In response to the quantum threat, the cryptographic community is actively developing post-quantum cryptographic algorithms. These algorithms are designed to withstand quantum attacks, ensuring the long-term security of encrypted data. Examples include lattice-based cryptography, hash-based cryptography, and multivariate polynomial cryptography.

Quantum-Resistant Blockchain Protocols

The integration of quantum-resistant cryptography into blockchain protocols is crucial for the sustained security of cryptocurrencies. Several blockchain projects are already exploring or implementing quantum-resistant solutions. These projects prioritize the development and adoption of quantum-resistant cryptographic algorithms, securing their networks against potential future quantum threats.

Future Prospects and Challenges

Ongoing Research in Quantum-Safe Blockchain Technology

The intersection of quantum computing and cryptocurrency security is a dynamic field with ongoing research initiatives. Collaborations between quantum experts and blockchain developers aim to create robust solutions that can withstand the computational power of quantum computers. Continuous research is essential to stay ahead of potential threats.

Regulatory Considerations and Standards

With the imminent challenge posed by quantum advancements, regulatory bodies are increasingly ac-

knowledging the significance of quantum-resistant cryptography. The establishment of standards for quantum-safe blockchain technology emerges as a critical step in guaranteeing a consistent and secure evolution within the cryptocurrency ecosystem. Regulatory guidance plays a pivotal role in incentivizing the widespread adoption of quantum-resistant solutions throughout the industry, fostering a resilient and future-proof environment for digital assets.

Potential Timeline for Integration

The seamless integration of quantum-resistant solutions into the cryptocurrency ecosystem hinges on the pace of advancements in quantum computing and the preparedness of cryptographic alternatives. Despite the potential advent of quantum computers with the capability to breach current cryptographic systems still being years away, the cryptocurrency community faces the imperative of proactive action. Implementing robust quantum-resistant measures now is essential to fortify the security of digital assets in anticipation of the imminent evolution in quantum technology.

Conclusion

In summary, the potential threats posed by Shor's algorithm and Grover's algorithm underscore the need for robust solutions in safeguarding the cryptographic foundations of cryptocurrencies. Fortunately, the ongoing development of quantum-resistant cryptography and its incorporation into blockchain protocols presents a promising avenue for ensuring a secure digital future. As the cryptocurrency landscape navigates these challenges, collaboration among quantum experts, cryptographers, and regulatory bodies becomes pivotal. To stay ahead in this dynamic environment, individuals and stakeholders are encouraged to explore forward-thinking options, such as the Bitcoin Era, which aligns seamlessly with the principles of quantum-resistant cryptography. The proactive adoption of such innovations will play a crucial role in determining the resilience of digital assets in the face of quantum advancements.

7.Experts divided over claims of 1st `practical' algorithm to protect data from quantum computers

by Keumars Afifi-Sabet
https://www.livescience.com/technology/computing/experts-divided-over-claims-of-1st-practical-algorithm-to-protect-data-from-quantum-computers

LaV's creators claim it's the first practical algorithm that can replace current-day encryption as the industry inches closer to creating a large-scale quantum computer.

Scientists think they've created the first practical cryptographic algorithm that could protect data and communications from quantum computers.

However, other experts in the field remain skeptical, saying algorithms backed by a cutting-edge U.S.-government-funded lab have a better chance of being used widely.

Cryptography tools, like WhatsApp's end-to-end encryption, protect data — like messages sent between two people — by scrambling it into a secret code that only a unique digital key can unlock. If hackers intercept an encrypted message, all they'll see is jumbled-up nonsense. The hacker could try to

guess the cryptographic key and decipher the message, but it would take the most powerful supercomputer millions of years to try every possible combination — which these machines would perform one at a time.

Quantum computers, on the other hand, can perform several calculations at once. They aren't powerful enough to break cryptography yet, but scientists plan to develop increasingly powerful machines that could one day bypass this essential security layer within seconds.

Now, researchers say they've developed the most efficient quantum-safe proposal to date, based on existing so-called verifiable random function (VRF) technology, which they dub "LaV." They described their research in a paper, which has not yet been peer-reviewed, published Nov. 14 in the Cryptology ePrint Archive, a cryptology research preprint database.

VRF takes a series of inputs, computes them, and churns out a random number that can be cryptographically verified to be random. It's usually an add-on to encryption that boosts the security of digital platforms. It's an essential part of WhatsApp's key transparency protocol, as well as some blockchain systems.

But LaV is a quantum-safe version of VRF. Unlike its predecessor, it could theoretically provide end-to-end security from quantum computers, said lead researcher Muhammed Esgin, an information technology lecturer at Monash University in Australia.

"Our algorithm is designed to withstand theoretical and practical attacks even by large-scale quantum computers (that can break today's classical cryptographic algorithms)," Esgin told Live Science in an email. "So it can protect against today's supercomputers as well as tomorrow's powerful quantum computers."

Will LaV be a quantum-safe game changer?

LaV can be accessed through the open-source platform GitLab. Its creators claim it's a practical solution, as opposed to four candidates backed by the National Institute of Standards and Technology (NIST), which has been hunting for a quantum encryption protocol for years. However, some experts disagree.

LaV may not be the best solution to the impending quantum threat, Edward Parker, a physical scientist with The RAND Corporation, told Live Science.

"There are several existing quantum-secure cryptography algorithms that already exist," he said, and NIST is standardizing these tools, "essentially giving those four algorithms the U.S. government's stamp of approval for widespread use."

"It's widely expected that these four algorithms will become the backbone of future quantum-secure cryptography, rather than LaV or any of the dozens of other quantum-secure algorithms that have been proposed," he added. "The four algorithms that NIST selected have undergone several years of very careful vetting, and we can be very confident that they are indeed secure."

Jonathan Katz, a computer scientist at the University of Maryland's Institute for Advanced Computer Studies (UMIACS), also backsNIST's efforts. "The cryptography research community has been working on quantum-safe algorithms for well over two decades, and the NIST post-quantum cryptography standardization effort began in 2017," he told Live Science in an email.

However, Parker added that "it's certainly possible that LaV may be somewhat more efficient than other quantum-secure algorithms."

Vlatko Vedral, a professor of quantum information science at the University of Oxford, told Live Science he suspects LaV may not be the first algorithm of its type, though it may be the first released publicly.

"The industry is getting closer and closer to making a large-scale quantum computer, and it is only natural that various protections against its negative uses are being explored," Vedral said. "Code making and code breaking have always been locked into an arms race against each other."

8.Dell expects quantum computing and generative AI to link in 2024

by Leigh Mc Gowran
https://www.siliconrepublic.com/enterprise/dell-tech-trends-2024-quantum-computing-generative-ai

Dell predicts that generative AI will move from theory to practice, powerful PCs will unlock more AI advancements and zero trust will become central to cybersecurity practices.

Dell Technologies Ireland MD Catherine Doyle has shared predictions on how technological advancements will impact businesses in 2024.

While AI was certainly one of the hottest topics of 2023, Doyle believes generative AI will be the “centre of business focus” and that 2024 will be “all about putting AI into action”.

“The first step on the AI journey should be to organise and structure data which will help avoid AI sprawl,” Doyle said.

Last year, the company made five predictions for 2023 that included advancements in AI, quantum computing and a greater role for technology in employee satisfaction.

Dell believes these advanced technologies will remain a central focus next year, but also believes zero-trust technologies and a growing focus on sustainability in IT will help organisations to innovate, enhance productivity and remain secure.

“Breakthrough technologies will help Irish businesses to navigate new challenges that may emerge in the coming months and to innovate at speed,” Doyle said.

Here are five predictions Dell has shared on how technology will advance in 2024.

Generative AI will take centre stage and move from theory to practice

Doyle said that 2023 saw various creative ideas on how generative AI will transform businesses, but claimed that there are “very few real-world examples” of generative AI in action.

“As we enter 2024, [generative] AI projects will start to be business ready with visible productivity gains becoming evident,” Doyle said. “An increasing number of Irish businesses will adopt AI and scale it across their organisations.”

Earlier this year, a State of IT report from Salesforce suggested that 91pc of Irish IT leaders believe generative AI will have a prominent role in their organisations in the near future. However, there also appeared to be feelings of caution, as 53pc of leaders said they were concerned about the ethics of gener-

ative AI.

Doyle said a recent report from Dell also suggests many Irish businesses are looking to integrate generative AI.

“According to our latest GenAI Pulse survey, nearly half of IT leaders expect to see meaningful results from [generative] AI initiatives within six months to a year,” Doyle said. “One of the first steps that leaders can take to ensure successful AI adoption in the year ahead is to organise and structure data within their business.”

Quantum computing and generative AI will become intertwined

Quantum computing has had some interesting developments this year, with some leaders claiming that the sector is moving at “breakneck speed” as interest grows among customers, investors and governments.

Doyle said that the growing demand for data will present an opportunity in the near future for quantum computing and generative AI to become closely linked.

“With the global explosion of data and AI, there will be an increasing need for organisations in Ireland to put in place the computing power to manage it effectively,” Doyle said. Quantum computing will begin to address this and bring about a massive leap in the computing power that is required to unlock AI innovation.

“If we were surprised by the [generative] AI advancements of the last year, leaders should expect to see a bigger jump forward when quantum computing becomes intertwined in the near future.”

AI will ‘come to life’ in more powerful PCs

Doyle also predicts that the promise of powerful digital assistants will become a reality next year, as PCs and AI technology become more powerful.

“Over the next 12 months the PC experience will shift from searching to prompting, from reading to understanding and from editing to directing,” Doyle said. “This will result in the emergence of a two-way human-machine partnership in workplaces across Ireland.

“Also, as AI becomes a key part of laptops and devices, it will unlock improved privacy and security while also advancing sustainable design.”

Zero trust will become central to cybersecurity

Zero trust is a modern cybersecurity strategy that is easy to understand based on the term – following a belief to never trust and always verify. Doyle believes 2024 will see zero-trust cybersecurity evolve from a “concept to a real technology”.

“Adopting a zero-trust approach helps organisations build a more resilient and responsive security infrastructure while ultimately lessening the impact of cyberattacks,” Doyle said. “As the benefits of zero-trust technology becomes evident, it is expected that zero trust will become the norm in a wider range of industries in Ireland.”

A greater adoption of green tech

Some experts argue that technology is one of the key ways companies and the wider community can achieve their sustainability goals. Luis Neves, the CEO of Global Enabling Sustainability Initiative, recent-

ly told SiliconRepublic.com that digital technologies will play a vital role in tackling the climate crisis and "broader sustainability issues".

Doyle predicts that the role played by technology in advancing sustainability will grow in 2024.

"With larger companies being required by the EU to disclose their environmental, social and governance (ESG) performance and activity, business and IT leaders in Ireland will increasingly rely on technology to track their climate data and reduce emissions," Doyle said.

"Our latest Digital Pulse Survey revealed that almost half of companies are looking at upgrading technology in the coming year to cut rising energy costs and drive sustainable innovation.

9.Preparing for Post-Quantum Risk: Quantum Cybersecurity in 2024

by Berenice Baker
https://www.iotworldtoday.com/security/preparing-for-post-quantum-risk-quantum-cybersecurity-in-2024

The awareness of quantum computing in 2023 was as much driven by the stick of the threat to public key encryption from near-future quantum computers as the carrot of use-case opportunities.

Even before quantum computers are powerful enough to break current encryption standards, threat actors are stealing vast amounts of encrypted data to decrypt at a later date. This activity is known as "harvest now, decrypt later."

But quantum technologies also offer solutions in terms of ultra-secure communication and quantum key distribution.

Enter Quantum has collected quantum cybersecurity predictions from experts to find out what to expect in the coming year and how to defend against the quantum threat to secure data.

Cambridge Consultants associate director of quantum algorithms James Cruise

The game-changing event expected in 2024 will be the final standardization of post-quantum cryptography (PQC) algorithms by NIST, expected sometime between March and June. This will finally open the floodgates on industry activity to put compliant PQC tech on the market –there have been plenty of prototypes, but without the finalized standard most things have been held back from volume production.

It will also start the clock on the US federal uptake of PQC solutions – Biden's National Security Memorandum 10 requires a timeline for the deprecation of non-PQC crypto in federal systems to be published within 90 days of the release of the standards.

Early adopters have already made significant strides on the PQC transition, including Cloudflare and Google Chrome. Since Chrome version 116, PQC algorithms have been available for testing, and in the latest release, Chrome 120, if you connect to Cloudflare or another compatible service, PQC will now be used by default under the hood.

The final standardization will enable such early adopters to make prototype services mainstream. However, the impact on many will be low as changes will happen in the background with little impact on users. Further, it is expected to take a few years before mainstream adoption of PQC in IoT devices occurs.

There will be a whole range of legacy technologies that cannot be upgraded and for which there are no PQC replacements. These will remain vulnerable and potentially become an issue if still in use when the quantum computing threat materializes. Security strategies for new products and services should incorporate concepts such as crypto agility to maximize the opportunity to defend against current threats, such as harvest now, decrypt later attacks, as well as future ones.

Qrypt CTO and co-founder Denis Mandich

The harvest now, decrypt later attack methodology is one of the highest potential payouts because the cost of storage is so minimal, and the possible financial value is so high. Therefore, cybercriminals will continue to target low-level access points, as they pay dividends as the entry operation to high-value assets over time.

Industries with the most monetizable data, including finance, healthcare, government and critical infrastructure – electricity, water, petroleum – will continue to be the industries with the highest risk of data stealing attacks in 2024 and beyond.

As the new Securities and Exchange Commission cybersecurity reporting rules hold chief information security officers (CISO) more responsible for cyber incidents and the number of fraud cases rises, CISOs and cybersecurity leaders will need to closely monitor systems for harvest now, decrypt later attacks and consider the potential security, business and regulatory repercussions.

Thales global head of data security products Todd Moore

Enterprises will finally grasp the importance of being quantum-ready in 2024. It will take standards to be agreed upon to finally get there – these are expected in 2024. But we will start to see interest in quantum computing break out of the technical circles it's largely languished in until now and onto the agenda of mainstream enterprise decision-makers in 2024.

Public key infrastructure, transport-later security encryption, browsers and code signing are the four essential areas where we will see greater interest in post-quantum cryptography in the coming year, not just in terms of mitigating risk, but as a business differentiator too.

10.Tiempo Secure's Unique IP Expertise Required to Secure First Post Quantum Sovereignty Chip

https://www.design-reuse.com/news/55446/tiempo-secure-post-quantum-sovereignty-chip.html

Tiempo Secure is proud to announce that we were selected to work on the µPQRS (Post Quantum, Secure, Resilient, and Sovereign Security Microprocessor) project, sponsored by the French State. Cybersecurity plays a key role in Europe's economic security at the advent of new post-quantum challenges

for attack protection. The Cyber Resilience Act introduces new European Union cybersecurity rules and requirements to improve the level of security of all hardware and software used in digital products, from the design and development phase right through their complete life cycle. Tiempo Secure has been working behind the scenes and leveraging its unique know-how and expertise, to test viable solutions in response to this strategic sovereignty issue.

The goal of the µPQRS project is to develop an innovative flexible security chip based on the RISC-V architecture, consisting of two subsystems – a low-power secure enclave and a high-performance microprocessor unit (MPU), for Eviden's data encryption products. Both subsystems will work concurrently to address the most demanding secure applications, including banking, electronic identity, government, defense, etc. By using a set of quantum-resistant cryptographic algorithms, the secure enclave will manage the secure boot and guarantee continued security levels while the MPU manages the applications and the surrounding execution environment.

The secure enclave will also act like an integrated hardware security module (HSM), providing cryptographic services to the MPU. The chip will include an embedded field programmable gate array (eFPGA), to manage future evolutions of cryptography standards and/or new I/O interfaces. The secure enclave will be capable of managing these evolutions and will provide security for the complete life cycle of the chip, in addition to test and debugging interference protection. This specific secure enclave will be designed to reach a Common Criteria EAL5+ certification level.

The µPQRS project represents an overall budget of €10 million and it received financial support from the French Public Investment Bank – Bpifrance. In line with Bpifrance's policy to support French sovereignty in strategic industry sectors, all the private and public stakeholders in the project are French. This ensures the safeguarding of technology for strategic French civil and defense applications.

Marc Renaudin, Tiempo Secure's co-founder, and Chief Technology Officer commented, "*We are very proud to be part of the µPQRS project, which confirms our commitment to French sovereignty initiatives. In addition, we will leverage this project to further develop our expertise in architecture design, to increase the reliability and performance levels of our secure solutions*".

The µPQRS project consortium includes:

- *Tiempo Secure* – a pre-certified embedded Secure IP provider
- *Eviden*, an Atos business – a leading provider of data encryption products
- *Menta*, a specialist in eFPGA
- *Synacktiv* – an expert in offensive cyber security
- *Institut Fourier* – a mathematics laboratory at Grenoble University, focusing on pre and post-quantum cryptography/computing
- *LIRMM* – a computer science, robotics, and microelectronics laboratory in Montpellier, focusing on trojan horse detection

11.QuSecure Introduces Post-Quantum Cryptography Cybersecurity Software QuProtect on AWS Marketplace

by Ray Sharma

https://www.thefastmode.com/technology-solutions/34372-qusecure-introduces-post-quantum-cryptography-cybersecurity-software-quprotect-on-aws-marketplace

QuSecure has announced the availability of its cutting-edge cybersecurity software **QuProtect** in the AWS Marketplace. The immediate availability of QuProtect on the trusted AWS Marketplace extends the reach of QuSecure's advanced enterprise security software solution to organizations of all sizes seeking robust protection against emerging cyber threats.

QuSecure is designed to safeguard sensitive and valuable information in an era where AI and quantum computing pose unprecedented risks to traditional encryption methods. By making QuProtect PQC web application security accessible in AWS Marketplace, QuSecure empowers organizations to fortify their digital defenses easily and seamlessly.

12.Chips to Compute With Encrypted Data Are Coming

by Samuel K. Moore
https://spectrum-ieee-org.cdn.ampproject.org/c/s/spectrum.ieee.org/amp/homomorphic-encryption-2666495720

Trust no one. It's not just a throwaway line from TV thrillers. It's becoming the goal of computer security, and a technology that can make it a reality has arrived. Called fully homomorphic encryption, or FHE, it allows software to compute on encrypted data without ever decrypting it.

The possibilities are enormous: huge leaps in medical research and patient care without exposing patient data, more effective tools against money laundering without regulators actually seeing anyone's bank-account information, self-driving cars that can learn from each other without snitching on their drivers, analytics about your business without poking into your customer's "business," and much more.

Although FHE software has made some inroads in protecting financial and health care data, it's been held back by the fact that it can take as much as a millionfold more effort on today's computers. But in 2024, at least six companies will be testing or even commercializing the first chips that accelerate FHE to the point where computing on encrypted data is nearly as quick as computing on unencrypted data. And when that's the case, why would you do it any other way?

"I think this is the coolest technology of the last 20 years," says Todd Austin, a hardware security expert at the University of Michigan, whose startup Agita Labs does a different form of secure computing in the Amazon and Microsoft clouds. "It breaks the cardinal rule of computer security—that everything is hackable—because you deny the programmer the ability to see the data."

Data Protection Regulations Aren't Enough

Regulatory efforts to protect data are making strides globally. Patient data is protected by law in the United States and elsewhere. In Europe the General Data Protection Regulation (GDPR) guards personal data and recently led to a US $1.3 billion fine for Meta. You can even think of Apple's App Store policies against data sharing as a kind of data-protection regulation.

"These are good constraints. These are constraints society wants," says Michael Gao, founder and CEO of Fabric Cryptography, one of the startups developing FHE-accelerating chips. But privacy and confi-

dentiality come at a cost: They can make it more difficult to track disease and do medical research, they potentially let some bad guys bank, and they can prevent the use of data needed to improve AI.

“Fully homomorphic encryption is an automated solution to get around legal and regulatory issues while still protecting privacy,” says Kurt Rohloff, CEO of Duality Technologies, in Hoboken, N.J., one of the companies developing FHE accelerator chips. His company’s FHE software is already helping financial firms check for fraud and preserving patient privacy in health care research.

Despite the relatively slow pace of today’s unaccelerated FHE, it works because “we address use cases where it’s not really a computation bottleneck, use cases where there is a human in the loop,” such as lawyers negotiating data-use agreements, Rohloff says. Adding a new kind of hardware to his company’s software won’t just speed FHE, it will let it tackle bigger human-in-the-loop problems as well, he says.

How Fully Homomorphic Encryption Works

At first glance, it might seem impossible to do meaningful computation on data that looks like gibberish. But the idea goes back decades, and was finally made possible in 2009 by Craig Gentry, then a Stanford graduate student. Gentry found a way to do both addition and multiplication without calculation-killing noise accumulating, making it possible to do any form of encrypted computation.

One comparison you can use to understand FHE is that it’s analogous to a Fourier transform. For those of you who don’t remember your college signal processing, a Fourier transform is a mathematical tool that turns a signal in time, such as the oscillation of voltage in a circuit, into a signal in frequency. One of the key side effects is that any math you can do in the time domain has its equivalent in the frequency domain. So you can compute in either time or frequency and come up with the same answer.

The genius of fully homomorphic encryption is that it uses lattice cryptography— a form of quantum-computer-proof encoding—as the mathematical transformation. The problem with this approach is that the transformation leads to a big change in the type and amount of data and in the sorts of operations needed to compute. That’s where the new chips come in.

Computing with FHE means doing transforms, addition, and multiplication on “a very long list of numbers, and each number in itself is very large,” explains Rohloff. Computing with numbers that might require more than a hundred bits to describe is not something today’s CPUs and GPUs are inherently good at. If anything, GPUs have been going in the opposite direction, focusing on less precise math done using smaller and smaller floating-point numbers. The FHE accelerator chips, by contrast, can stream huge volumes of data through hardware that does integer math on numbers that are thousands of bits long to accommodate encryption’s precision needs.

Each accelerator has its own way of dealing with these streams of huge numbers. But they’re all after the same goal—making FHE as fast as today’s unencrypted computing.

DARPA Drives FHE

The quest for hardware that can accelerate FHE got its biggest boost in 2021, when the U.S. Defense Advanced Research Projects Agency (DARPA) began a project called DPRIVE. The goal was to build hardware that could radically reduce the time it took for FHE computing tasks, from weeks to just seconds or even milliseconds. Three participating teams—led by Duality Technologies, Galois, and Intel—are on track to deliver chips designed to make FHE perform within a factor of 10 of traditional computing or even better in 2024.

These chips will be crucial if FHE is to break out of its current niche. “While algorithm and software development has taken us far, it’s not nearly far enough for FHE to be practical in any but a small and narrow set of applications,” says Galois’s David Archer. A distinction of the Galois hardware,

called Basalisc, is the use of asynchronous clocking so that the various types of circuits used to do FHE operations can run at their own speed.

For the Intel team's chip, Heracles, they came up with a way to decompose FHE's huge numbers into short data words that are just 32 bits. The smaller words lead to a lower computing latency. They also mean Intel can squeeze in more computational units and more pathways for data to reach those units, explains Ro Cammarota, chief scientist for privacy-enhanced computing research at Intel.

The Duality team, whose chip is called Trebuchet, sees its advantage as having a design that's made to support and accelerate the FHE software the startup has already commercialized. "We started from applications to drive our software and then have that software drive our hardware," says Rohloff.

FHE Startups Smell Opportunity

At least three other companies went after FHE hardware independently of DARPA's DPRIVE.

Gao founded Fabric Cryptography after leaving his previous startup, an optical computing company called Luminous that sought to accelerate AI. Impressed and a little concerned with the amount of data his customers had, Gao wanted to see what encrypted computing could do about maintaining people's privacy while still helping businesses benefit from the information. The result is a chip that Fabric expects to be in mass production within the year.

For Campbell, Calif.–based Cornami, FHE was an opportunity to repurpose a new type of parallel computing architecture. The architecture was originally designed to speed computing by allowing programs to be broken up into completely independent streams of instructions, which could then flow through the processor's many cores without the delays of having to share resources.

When chip-industry veteran Walden C. "Wally" Rhines came across Cornami in 2019, the company was planning to apply the architecture to machine learning, but the field was already too crowded, he says. Instead, fresh off some work for DARPA on FHE, he steered the startup in that direction. Rhines, who is now CEO, says Cornami will have a product ready in 2024 that will let FHE match plain-text computation speeds.

Optalysys, in Leeds, England, is looking to take advantage of optical computing's inherent agility with Fourier transforms. It's long been known that a fairly straightforward optical system can instantly produce the Fourier transform of a two-dimensional image. Optalysys was founded more than a decade ago to exploit this phenomenon, and it has built systems over the years for defense-related tasks like finding patterns in cluttered images.

With the increasing availability of silicon photonics tech, the company has been able to adapt its transform-powered technology for encryption and FHE, CEO Nick New says. "FHE is an area that is absolutely dominated by" transforms that can be done in optics, he says. The startup plans to have a product ready in the second half of 2024.

FHE's Road Ahead

"Ultimately, if it's fast enough and cost effective enough, there's no reason not to use FHE," says New. "But there's a long way to go to get to that point."

Intel's Cammarota sees the accelerator chips as just the starting point. FHE will also need software development tools to make programming easier as well as standardization. The two are in progress even without chips in hand, but there are many ways to do FHE and standardization work is in its early stages.

Once industry has all three ingredients—software, standards, and hardware—researchers can begin to

see what else these accelerator chips can do. “It’s a new chapter in the history of computing,” says Cammarota.

13.SKT and Thales partner to test quantum-resistant cryptography for 5G

https://www.vanillaplus.com/2023/12/20/85358-skt-and-thales-partner-to-test-quantum-resistant-cryptography-for-5g/

In the context of 5G networks and the evolution of cryptographic standards, **SK Telecom** (SKT) and **Thales** partnered to test advanced quantum-resistant cryptography. Based on the 5G standalone network and 5G SIM, the solution aims at encrypting and decrypting subscriber identity in a secure way to protect user privacy from future quantum threats. This achievement is already crucial today as it protects subscribers against potential ‘record now, decrypt later’ attacks.

It also represents a major step forward since it allows the safeguarding of subscribers’ identities using a regular commercial telecom network.

The innovation consists in upgrading the cryptography used to anonymise the user’s digital identity on the 5G network. Indeed, the user identity on a 5G network is concealed and secured on the device side thanks to the 5G SIM. The security mechanisms involve cryptographic algorithms designed to resist attacks from future quantum computers, providing a level of security that is considered robust in the post-quantum era.

The U.S. National Institute of Standards and Technology (NIST) has been leading an initiative to standardise post-quantum cryptographic algorithms, and SKT and Thales have used the Crystals-Kyber one for this real condition trial. These post-quantum secure algorithms are being developed to withstand attacks from both classical and quantum computers.

“This collaboration between SKT and Thales highlights our commitment to staying ahead of the curve in terms of cybersecurity and ensuring the safety of our customers’ data,” said Yu Takki, a vice president and head of infra technology office of SKT. “PQC provides enhanced security through the use of cryptographic algorithms that are thought to be secure against quantum computer attacks. Going forward, we will combine PQC SIM with our additional Quantum expertise to achieve end-to-end quantum-safe communications.”

“As quantum computers have the potential to break certain existing cryptographic algorithms, there is an emerging need to transition to cryptographic algorithms believed to be secure against quantum attacks,” said Eva Rudin, a senior vice president for mobile connectivity and solutions at Thales. “For 5G networks, Thales started to invest on cryptographic algorithms that are quantum-resistant to enhance continued communications security and privacy for users.

14.NSA Publishes 2023 Cybersecurity Year in Review

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3621654/nsa-publishes-2023-cybersecurity-year-in-review/

The National Security Agency (NSA) published its 2023 Cybersecurity Year in Review today to share its recent cybersecurity successes and how it is working with partners to deliver on cybersecurity advances that enhance national security. This year's report highlights NSA's work with U.S government partners, foreign partners, and the Defense Industrial Base.

"The combined talent of our partners is the greatest competitive advantage we have to confront the increasingly sophisticated threats we see today"- Rob Joyce, Director of Cybersecurity

The Cybersecurity Year in Review highlights NSA's recent cybersecurity efforts, including:

- Establishing the Artificial Intelligence (AI) Security Center.
- Detecting stealthy People's Republic of China (PRC) intrusions into U.S. critical infrastructure and joined forces with partners (CISA, FBI, NIST, etc.) to expose those intrusions.
- Collaborating with industry, government stakeholders, and academia to modernize cryptography to scale cybersecurity solutions and address the quantum threat.

"Cybersecurity matters. It matters to our partners and it matters to us. It ensures that our information, our intelligence, our knowledge can be shared securely."- General Paul M. Nakasone, U.S Army; Commander, U.S Cyber Command; Director, National Security Agency; Chief, Central Security Service

This report includes information about NSA's cybersecurity partnerships and the efforts in building them. This year NSA:

1. Inaugurated the new AI Security Center within the Cybersecurity Collaboration Center, which will promote the secure development, integration, and adoption of AI capabilities within National Security Systems (NSS) and the Defense Industrial Base (DIB).
2. Scaled NSA's cybersecurity impact against global threats like Russian cyberespionage malware and malicious cyber activity from the People's Republic of China together with U.S. and international partners and collaborators.
3. Increased enrollments in NSA's no cost cybersecurity services to Department of Defense contractors by 400%, hardening infrastructure and strengthening the Defense Industrial Base.

15.Deloitte predicts 2024 will be a breakthrough year for post-quantum cryptography

by Nancy Liu
https://www.sdxcentral.com/articles/analysis/deloitte-predicts-2024-will-be-a-breakthrough-year-for-post-quantum-cryptography/2023/12/

Deloitte's managing director of risk and financial advisory Colin Soutar anticipates that in 2024, "post-quantum cryptography (PQC) will come of age," driven by the upcoming PQC standard release from the National Institute of Standards and Technology (NIST). Organizations across various sectors, led by federal and financial entities, are preparing for this transition. Soutar also shed light on the expanding ecosystem of PQC vendors and the role they play in this transition.

More organizations advance toward quantum readiness

"Drafts of PQC standards have recently been released and with that, in 2024, I expect that we will see a new group of organizations begin to take steps towards quantum readiness – starting with assessments of their cryptographic exposure – while those who have already commenced that journey will add further to their cryptographic agility plans," Soutar noted in his predictions.

The three draft PQC standards NIST released earlier this year include the Module-Lattice-based Key-Encapsulation Mechanism Standard, Module-Lattice-based Digital Signature Standard and Stateless Hash-Based Digital Signature Standard. A fourth standard derived from Falcon is expected to be released soon and the institute expects to finalize its PQC standards by 2024.

Potential PQC regulations

It's uncertain whether regulators will immediately adopt and mandate the use of the NIST Federal Information Processing Standards (FIPS) upon release of the PQC standards, or delay the implementation, Soutar told SDxCentral.

"I think in the federal environment, there's an immediate connection to what they have to do," he said, adding that for commercial entities, particularly those that are deemed within critical infrastructure, it would be very interesting to watch if they are going to adopt the standards immediately and some industries may wait for regulations to adopt PQC.

"From our perspective, we are cautious about that being a driver for adoption of the PQC standards, because the regulators may wait for more of a commonplace, linear set of activities, whereas quantum computing almost by its very nature, it's not linear, and we don't know how quantum computing may mature more rapidly than people had thought," Soutar said.

Instead, he suggests organizations both in the federal and commercial spaces should take action to understand their potential post-quantum threat exposure, conduct an inventory of existing cryptographic systems and assets, learn how to adopt the upcoming PQC standards, aiming for crypto agility or maybe a classic and post-quantum hybrid cryptosystem in the future.

Industries at the quantum-readiness forefront

Regarding the industry readiness for quantum computing, the U.S. federal sector and other governments around the world are leading, followed by the financial sector. Some large financial institutions are proactively assessing their exposure and potential market advantages, Soutar said.

Healthcare, technology vendors especially the hyperscalers like Google, Amazon Web Services and Microsoft, telecommunications and space operation sectors are also becoming aware of the need for quantum readiness, he added.

The expanding PQC vendor landscape

"In addition, the continued expansion in the number and capabilities of PQC vendors will help organizations' programs to improve by offering a greater ability to upgrade cryptographic algorithms across vast, heterogeneous environments," Soutar forecasts.

He categorizes **PQC vendors into three categories:** **hyperscalers** or large cloud service providers; **traditional security** vendors that started to look at post-quantum threats, **PQC** or have been working in public key infrastructure; and specialized vendors that have been established because of the post-quantum threats.

Cybersecurity vendors and PQC services

Soutar expects more traditional security vendors to add post-quantum services to their portfolio. “They have a more nuanced understanding of quantum. And a lot of the discovery services that are being done tend to be similar across the vendors these days.”

However, more quantum-specialized vendors have unique expertise in PQC algorithms, quantum computer developments, and quantum-derived technologies like quantum key distribution and quantum random number generation, he said.

Selecting the right PQC vendor

Choosing a PQC vendor requires a tailored approach. Soutar said Deloitte helps clients navigate this post-quantum transition process.

“We offer services similarly around the discovery of the algorithms that are there, working on roadmaps in terms of transition. And then if there are particular technologies that can be pulled through, we often work with the client in terms of what their specific needs are, and we can help them make that decision themselves based on the different aspects that they’re looking for,” he said.

16.U.S. and China race to shield secrets from quantum computers

by David Lague
https://www.reuters.com/investigates/special-report/us-china-tech-quantum/

The encryption guarding digital communications could someday be cracked by quantum computers. Dubbed `**Q-day**,' that moment could upend military and economic security worldwide. Great powers are sprinting to get there first.

In February, a Canadian cybersecurity firm delivered an ominous forecast to the U.S. Department of Defense. America’s secrets — actually, everybody’s secrets — are now at risk of exposure, warned the team from Quantum Defen5e (QD5).

QD5’s executive vice president, Tilo Kunz, told officials from the Defense Information Systems Agency that possibly as soon as 2025, the world would arrive at what has been dubbed “Q-day,” the day when quantum computers make current encryption methods useless. Machines vastly more powerful than today’s fastest supercomputers would be capable of cracking the codes that protect virtually all modern communication, he told the agency, which is tasked with safeguarding the U.S. military’s communications.

In the meantime, Kunz told the panel, a global effort to plunder data is underway so that intercepted messages can be decoded after Q-day in what he described as “harvest now, decrypt later” attacks,

according to a recording of the session the agency later made public.

Militaries would see their long-term plans and intelligence gathering exposed to enemies. Businesses could have their intellectual property swiped. People's health records would be laid bare.

"We are not the only ones who are harvesting, we are not the only ones hoping to decrypt that in the future," Kunz said, without naming names. "Everything that gets sent over public networks is at risk."

Kunz is among a growing chorus sounding this alarm. Many cyber experts believe all the major powers are collecting ahead of Q-day. The United States and China, the world's leading military powers, are accusing each other of data harvesting on a grand scale.

The director of the Federal Bureau of Investigation, Christopher Wray, said in September that China had "a bigger hacking program than every other major nation combined." In a September report, China's chief civilian intelligence agency, the Ministry of State Security, accused the U.S. National Security Agency of "systematic" attacks to steal Chinese data.

The National Security Agency declined to comment on China's accusation.

More is at stake than cracking codes. Quantum computers, which harness the mysterious properties of subatomic particles, promise to deliver breakthroughs in science, armaments and industry, researchers say.

Opinion is divided on the expected arrival of Q-day, to be sure. It's still relatively early days for quantum computing: So far, only small quantum computers with limited processing power and a vulnerability to error have been built. Some researchers estimate that Q-day might come closer to the middle of the century.

No one knows who might get there first. The United States and China are considered the leaders in the field; many experts believe America still holds an edge.

As the race to master quantum computing continues, a scramble is on to protect critical data. Washington and its allies are working on new encryption standards known as post-quantum cryptography – essentially codes that are much harder to crack, even for a quantum computer. Beijing is trying to pioneer quantum communications networks, a technology theoretically impossible to hack, according to researchers. The scientist spearheading Beijing's efforts has become a minor celebrity in China.

Quantum computing is radically different. Conventional computers process information as bits — either 1 or 0, and just one number at a time. Quantum computers process in quantum bits, or "qubits," which can be 1, 0 or any number in between, all at the same time, which physicists say is an approximate way of describing a complex mathematical concept.

These computers also exploit a mysterious property of quantum mechanics known as entanglement. Particles such as *photons* or *electrons* can become entangled so that they remain connected, even when separated by huge distances. Changes in one particle are immediately reflected in the other. The properties of qubits and entanglement are fundamental to quantum computers, say physicists and computer scientists, potentially allowing calculations to be carried out that would be impractical on today's large supercomputers.

Business consultants forecast this processing power will deliver hundreds of billions of dollars in extra revenue by the middle of the next decade. Even before these computers arrive, some are predicting that advances in quantum technology will sharply improve the performance of some military hardware.

Quantum technology "is likely to be as transformational in the 21st century as harnessing electricity as a

resource was in the 19th century," said Michael Biercuk, founder and chief executive officer of Q-CTRL, a quantum tech company that was established in Australia and has major operations in the United States.

It was the codebreaking possibilities of quantum computing that sparked the field's surge in progress in recent decades, said Q-CTRL's Biercuk, an American who is a professor of quantum physics at the University of Sydney and a former consultant to the U.S. Defense Advanced Research Projects Agency, the Pentagon's innovation incubator. The U.S. government saw it as a "big opportunity " in the 1990s and has been funding research ever since, he said.

In his briefing for the Pentagon, QD5's Kunz cited what he called one of the most successful harvest now/decrypt later operations ever: the Venona project.

Launched in 1943, Venona was a 37-year U.S. effort to decipher Soviet diplomatic communications collected by the Americans during and after World War Two. U.S. codebreakers, aided by allies, were able to decrypt more than 2,900 cables from thousands of messages sent by Soviet intelligence agencies between 1940 and 1948, according to CIA documents.

The cables revealed extensive Communist intelligence operations against the United States and its allies. The code-cracking coup led to the discovery of Soviet penetration of the Manhattan Project, the top-secret program to build the first atomic bombs, and the existence of the Cambridge Five, a group of top British civil servants spying for Moscow, the CIA documents show.

The West's breakthrough was the realization that the Soviets had misused so-called one-time pads: a time-tested form of encryption in which a secret key is used to encode a message sent between parties. The method got its name because in its earliest forms, keys were printed on a pad whose pages each contained a unique code; the top page was ripped off and destroyed after a single use. The Soviets blundered by printing and using duplicate pages in one-time pads for a limited time. This allowed allied analysts to painstakingly decrypt some of the messages years later, according to the CIA documents.

To be truly unbreakable, cybersecurity experts say, a one-time-pad key must be a set of random numbers equal to or bigger than the size of the message – and used only once. The party receiving the message uses the same secret key to decrypt the message. The method was invented more than a century ago, and for decades was used for secret messages by most major powers. But technical factors made it too unwieldy for mass, secure communication in the modern era.

Instead, most communications today are secured with what is known as public key infrastructure (*PKI*), a system developed in the 1970s to enable encryption on a mass scale.

PKI enabled the rise of the internet economy and open telecommunications systems. The passwords to email accounts, online banking and secure messaging platforms all rely on it. PKI is also critical to most government and national security communications.

Security provided by PKI stems essentially from hiding information behind a very difficult math problem, Biercuk said. The most widely used algorithm that creates and manages that difficult math problem used for encryption is known as RSA, from the surname initials of its inventors: the computer scientists and cryptographers Ron Rivest, Adi Shamir and Leonard Adelman. What may be about to change is that these problems will be a cinch for quantum computers to solve.

"If you have a computer for which that math problem is not very hard," Biercuk said, "all of that is at risk."

Montreal-based QD5, the privately held company where Kunz is executive vice president, is taking a different approach to post-quantum cryptography. It has developed an advanced version of the one-time

pad: a device, the Q PAD, which it claims customers can use to conduct communications on existing networks that will remain uncrackable forever. Pentagon officials peppered Kunz and colleagues with technical questions about the technology in February, but noted the informational session didn't necessarily signal an intent to buy the Q PAD system.

The Defense Information Systems Agency did not respond to requests for comment.

In an interview, Kunz, a former Canadian soldier, said he first learned about one-time pads while serving with a reconnaissance unit.

"It is very simple and straightforward," he said. "Every time you used one of those sheets of paper, you would have to destroy it. If you only have those two keys, and follow the rules," a message may be intercepted, but the enemy "will never be able to break it."

QD5 has overcome some of the limitations of the original one-time pad, said Chief Technology Officer Gary Swatton. One hurdle to mass use of the method was the need to generate enough sets of truly random numbers to supply modern communications networks with encryption. Before quantum technologies emerged, this took considerable time and effort.

Now, specially designed semiconductor chips and hardware, called quantum random number generators, can exploit the truly random nature of subatomic quantum particles to generate number sets in large volumes, according to researchers. "Technology has caught up and is solving these problems," Swatton said.

Other companies hope to seize on demand for better security. SandboxAQ of Palo Alto, California, a spin-off from Google owner Alphabet, has a division to help clients tackle the threat from quantum computing and leverage the benefits of this powerful technology. Even if Q-day is a decade or more away, "it's imperative that organizations begin preparing for the migration to post-quantum cryptography now," said Marc Manzano, SandboxAQ's general manager of quantum security.

Some anticipate upheaval. Skip Sanzeri, founder and chief operating officer of quantum security company QuSecure in San Mateo, California, says "the entire internet and the devices connected to it" will be affected. The World Economic Forum has estimated that 20 billion devices will have to be upgraded or replaced to meet quantum security standards in the next two decades.

"This is going to be a $100 billion or trillion-dollar upgrade," Sanzeri says.

While quantum computing threatens to upend existing security measures, the physics behind this technology could also be exploited to build theoretically unhackable networks.

In a quantum communications network, users exchange a secret key or code on subatomic particles called photons, allowing them to encrypt and decrypt data. This is called quantum key distribution, or QKD. It is one of the fundamental properties of quantum mechanics that can ensure secure communications. Any attempt to monitor or interfere with these quantum particles changes them, physicists explain. That means any attempt to intercept the communications is immediately detectable to users. If the communicating parties receive an uncorrupted encryption key, they can be confident that their subsequent communications will be secure.

With quantum networks, "our technical security comes from the laws of physics," says physicist Gregoire Ribordy, chief executive officer of ID Quantique (IDQ), a privately held Swiss company that provides quantum communications technology. "Interception of the communications is just not possible without leaving a trace."

Quantum communications is an area where China is spending big. The technology has the potential to

safeguard Beijing's data networks, even if Washington and other rivals are first to reach Q-day.

President Xi Jinping stressed the "strategic value" of quantum technology in a 2020 speech to top Chinese leaders, the official Xinhua news agency reported. Under Xi, China has set clear targets to dominate quantum science. It is spending more than any other country on quantum research by some estimates. In an April report, McKinsey & Company estimated that Beijing had announced a cumulative $15.3 billion in funding for quantum research, more than quadruple the equivalent U.S. figure of $3.7 billion.

A key driver of China's quantum tech quest is **Pan Jianwei**, a physicist who has achieved celebrity status in China along with praise and support from the ruling Communist Party.

Pan, 53, is a professor at the University of Science and Technology of China, the country's premier quantum research outfit. In 2011, he was elected to the Chinese Academy of Sciences, an honor given to scientists who have made important advances in their fields.

Pan in media interviews has said he wants to make China a leader in quantum technology while building an internet secure from cyberattacks. This would serve vital strategic purposes, security experts say. It would protect the Chinese leadership and military from hacking, especially in a conflict. A quantum-fortified internet could protect vital infrastructure and the vast surveillance network the Communist Party has built to stamp out any challenge to its monopoly on power, they say.

Pan did not respond to requests for an interview.

Pan's career highlights how the absorption of foreign technology has been crucial to China in quantum and other tech fields.

He studied for his doctorate in Vienna with renowned physicist Anton Zeilinger. Zeilinger shared the 2022 Nobel Prize in Physics for his work on quantum mechanics. Pan later moved to the University of Heidelberg, where he still maintains close links, before returning home in 2008.

Zeilinger did not respond to a request for comment.

Back in China, Pan led a team that recorded a milestone in 2016 with the launch of Micius, the world's first quantum satellite, which was used to establish secure communications links with ground stations in China.

The following year, his team and researchers in Austria used Micius to hold the world's first quantum-encrypted teleconference, connecting Beijing and Vienna. Pan also led a team that has reportedly built a similarly unhackable ground-based network in China linking the cities of Beijing, Jinan, Shanghai and Hefei.

Pan was one of the architects of a concerted campaign to deploy Chinese scientists to leading quantum labs around the world, with the goal of jump-starting domestic development when these researchers returned home, according to a 2019 report by Strider Technologies, a Salt Lake City-based strategic intelligence startup.

Some of those researchers, including Pan, benefited from substantial foreign government funding while studying abroad, the report found. "From that regard it has been wildly successful," Strider Technologies Chief Executive Officer Greg Levesque said of the Chinese strategy in an interview with Reuters. "But I don't know if they are going to win it," he added. "It seems some U.S. companies are making some really big leaps."

Despite China's apparent lead in official funding, some researchers say America remains the overall

quantum leader thanks to its private sector technology innovators, government labs, university researchers and collaborating allies. And Washington is moving to restrict U.S. investment in China's quantum capabilities.

In August, President Joe Biden signed an executive order directing the U.S. Department of the Treasury to regulate U.S. investments in quantum computing, semiconductors and artificial intelligence. An annex to that order named China as a country of concern, along with its special administrative regions of Hong Kong and Macau. That could lead to bans on investment in Chinese production of quantum technologies and equipment.

China's Ministry of Foreign Affairs did not respond to a request for comment.

New security era

Globally, government security agencies and the private sector are working on strategies to beat quantum computers. In August, the U.S. National Security Agency and other agencies urged the public and companies to adopt new measures to safeguard their communications with post-quantum cryptography.

After extensive evaluation, the U.S. National Institute of Standards and Technology (NIST) last year selected four so-called post-quantum cryptography (PQC) algorithms – new encryption standards that some cyber experts believe will provide long-term security. U.S. government agencies next year are expected to issue a new standard for post-quantum cryptography, Biden disclosed in a May memo. NIST said in August that it's working on standardizing these algorithms, the final step before making these tools widely available for organizations to upgrade their encryption.

SandboxAQ's Manzano said his company is working with some of the world's biggest companies and government agencies to integrate the coming PQC cryptography algorithms into their systems. Sanzeri said QuSecure, too, is working with government and private clients to upgrade to PQC.

Not everyone agrees the new algorithms will offer reliable security. Kunz told Reuters that eventually the new cyphers could be compromised as quantum computers improve. "The problem is that PQC is not unbreakable," he said. "It does not solve the harvest now, decrypt later problem."

IDQ's Ribordy said that today's classical computers also might be able to crack these new codes. The complex math problems at the heart of PQC are "so new" that they have not been studied very extensively, he noted.

A spokesperson for NIST said the agency "has confidence in the security of the PQC algorithms selected for standardization, (or) else we wouldn't be standardizing them. The algorithms have been studied by experts, and went through an intensive evaluation process." He added that it was not inevitable or even a "safe assumption" that they would be broken.

The National Security Agency declined to comment on the PQC algorithms, referring Reuters to information on its website about quantum computing and post-quantum cryptography.

In the meantime, one challenge for the keepers of digital secrets is that whenever Q-day comes, quantum codebreakers are unlikely to announce their breakthrough. Instead, they're likely to keep quiet, so they can exploit the advantage as long as possible.

"We won't necessarily know" when the codes are broken, Kunz told the Pentagon panel. "We will probably find out the hard way," he said. "But what we can expect is that they will be broken."

17.Fostering Digital Trust – the role of 'post-quantum crypto' and 'crypto agility' in 2024

by Byron V. Acohido
https://www.lastwatchdog.com/my-take-fostering-digital-trust-the-role-of-post-quantum-crypto-and-crypto-agility-in-2024/

Notable progress was made in 2023 in the quest to elevate Digital Trust. Digital Trust refers to the level of confidence both businesses and consumers hold in digital products and services – not just that they are suitably reliable, but also that they are as private and secure as they need to be.

We're not yet at a level of Digital Trust needed to bring the next generation of connected IT into full fruition – and the target keeps moving. This is because the hyper interconnected, highly interoperable buildings, transportation systems and utilities of the near future must necessarily spew forth trillions of new digital connections.

And each new digital connection must be trustworthy. Therein lies the monumental challenge of achieving the level of Digital Trust needed to carry us forward. And at this moment, wild cards – especially generative AI and quantum computing — are adding to the complexity of that challenge.

I had the opportunity to sit down with DigiCert's Jason Sabin, Chief Technology Officer and Avesta Hojjati, Vice President of Engineering to chew this over. We met at DigiCert Trust Summit 2023.

We drilled down on a few significant developments expected to play out in 2024 and beyond. Here are my takeaways:

PKI renaissance

Trusted digital connections. This is something we've come to take for granted. And while most of our digital connections are, indeed, robustly protected, a material percentage are not; these range from loosely configured cloud IT infrastructure down to multiplying API connectors that many companies are leaving wide open, all too many APIs simply going unaccounted for.

Each time we use a mobile app or website-hosted service, digital certificates and the Public Key Infrastructure (PKI) come into play — to assure authentication and encrypt sensitive data transfers. This is a fundamental component of Digital Trust – and the foundation for securing next-gen digital connections.

The goal is lofty: companies and consumers need to feel very confident that each device, each document, and each line of code can be trusted implicitly. And PKI is the best technology we've got to get us there.

"PKI has been around for 30 years in lots of different reincarnations," Sabin noted. "We're hitting a massive resurgence, almost a renaissance of PKI right now, because there are so many use cases where the simple ingredients of PKI can be used very effectively to solve the business needs of today."

Enter the concept of "cryptographic agility" — a reference to the rise of a new, much more flexible ap-

proach to encrypting digital assets. Crypto agility has arisen because digital connections are firing off more dynamically than ever before. Thus companies increasingly require the ability to update encrypted assets in a timely manner and even switch them out as needed, Sabin says.

Post-quantum crypto

A high level of Digital Trust, one that leverages crypto agility, is needed for companies to thrive in environment where cyber attacks are becoming more targeted and severe – and with generative AI providing a great boon to the attackers.

What's more, a fresh layer of risks posed by the rise of quantum computing looms large. And this is were something called "post-quantum cryptography" (PQC) comes into play.

The National Institute of Standards and Technology (NIST) is in the late stages of formally adopting established standards for PQC; this will result in NIST-recommended encryption algorithms that can withstand potential threats posed by quantum computers.

Sabin pointed me to a recent Ponemon Institute polling of 1,426 IT security pros that reveals a worrying lack of PQC-readiness among companies across the US, Europe, the Middle East and Asia-Pacific. The survey found a skills shortage, budget constraints and uncertainty about PQC causing some 61% of respondents to acknowledge that their organizations are not prepared.

Yet quantum computing exposures are happening today. Threat actors are pursuing a "harvest now, decrypt later" strategy, Savin told me. They're hoarding stolen cyber assets encrypted with current day algorithms, he says, and patiently waiting for quantum hacking routines to emerge that will enable them to crack in.

PKI playground

To aid and abet the PQC transition, DigiCert has been collaborating with industry partners to develop encryption methods that can withstand the threats posed by quantum computing. DigiCert recently released the DigiCert PQC Playground — a part of DigiCert Labs designed to let security code writers and tech enthusiasts experiment with the NIST-endorsed PQC algorithms which are slated to go into effect in 2024.

Playground visitors can get in the practice of issuing certificates and PKI keys under NIST's three most advanced encryption algorithms: CRYSTALS-Dilithium, FALCON, and SPHINCS+. Hojjati told me this free tool is intended to be an incubator for development and innovation, demystifying PQC by providing a user-friendly environment for experimentation.

The aim is to alleviate apprehension surrounding the deployment of PQC algorithms and certificates, Hojjati says. This will give software developers, CISOs and other stakeholders a sandbox to test and understand the practical implications of integrating the new NIST algorithms into their systems, he says.

As standards and best practices solidify, a new senior leadership role — the Chief Digital Trust Officer — has cropped up. The office of CDTO is gaining traction in large enterprises that are proactively pursuing Digital Trust. These new security leaders are not just technologists, Sabin says, they are strategists and visionaries.

"In the last 18 months we're already seeing a number of companies create this new C-level role, recognizing that Digital Trust is critical to their capabilities, their business objectives and the vision of the company," Sabin says.

As we turn the corner into 2024, Digital Trust is in sight. I'll keep watch and keep reporting.

18.Rigetti Launches Novera QPU, The Company's First Commercially Available QPU

by Matt Swayne
https://thequantuminsider.com/2023/12/09/rigetti-launches-novera-qpu-the-companys-first-commercially-available-qpu/?utm_source=newsletter&utm_medium=email&utm_term=2023-12-23&utm_campaign=TQI+Weekly+Newsletter+--+Kipu+Quantum+Seeded+Catty+Error+Correction+Plus+More+Quantum+News+Industry+Updates

Rigetti Computing, Inc. (`Rigetti" or the ``Company"), a pioneer in full-stack quantum-classical computing, announced the launch of its Novera™ QPU, a 9-qubit quantum processing unit (QPU) based on the Company's fourth generation Ankaa™-class architecture featuring tunable couplers and a square lattice for denser connectivity and fast 2-qubit operations. The Novera QPU is manufactured in Rigetti's Fab-1, the industry's first dedicated and integrated quantum device manufacturing facility.

The Novera QPU includes all of the hardware below the mixing chamber plate (MXC) of a dilution refrigerator. In addition to a 9-qubit chip with a 3×3 array of tunable transmons, the Novera QPU also includes a 5-qubit chip with no tunable couplers or qubit-qubit coupling which can be used for developing and characterizing single-qubit operations on a simpler circuit. In addition to the 9-qubit and 5-qubit chips, Novera QPU components include:

- A puck that contains both the 9-qubit and 5-qubit chips, interposers and a PCB to route signals to SMPM connectors at the puck periphery.
- A tower that hangs from the MXC and connects coaxial cables between the puck and the SMA patch panel. The tower delivers cooling power from the MXC to the chips.
- Shields that surround the tower to isolate the puck from infrared radiation and stray magnetic fields.
- Payload brackets and a signal chain installed around the tower with mounted signal conditioning devices, including ferrite isolators, diplexers, filters, and optional quantum-limited amplifiers.

"Our new Novera QPU enables hands-on access to our most innovative quantum computing technology. With the same architecture as our 84-qubit Ankaa systems, researchers working with the Novera QPU can have a head start in pursuing their quantum computing work and drive the industry forward," says Dr. Subodh Kulkarni, Rigetti CEO. "Our Ankaa-class 9-qubit QPUs have already been commissioned by premier national labs, and now the same technology is available to those seeking to accelerate their own quantum computing work."

Fundamental research to gain a better understanding of how qubits operate, how to optimize control systems, testing how to design and characterize gates, ways to mitigate decoherence, and how to develop more efficient quantum algorithms are among the key focus areas for building higher quality quantum computers.

“With the launch of the Novera QPU, quantum computing professionals and students can now have on-premise access to years of Rigetti’s internal R&D within a matter of weeks. Rigetti has been pioneering full-stack quantum computing technology for 10 years. This is an exciting moment for us to equip the quantum computing ecosystem with the same caliber of hardware and engineering that we use on our most powerful QPUs,” says David Rivas, Rigetti CTO.

The Novera QPU implements universal, gate-based quantum computing and can be used by quantum software and algorithm experts to prototype and test: (1) hybrid quantum algorithms, (2) characterization, calibration, and error mitigation, and (3) quantum error correction (QEC) experiments.

Additionally, organizations looking to develop components of their quantum computing stack can leverage the Novera QPU to accelerate areas such as: (1) control electronics and software, (2) QEC decoders, (3) control optimization algorithms, (3) native gate architectures, and (4) measurement and calibration, and accompanying software.

The Novera QPU is designed to be integrated with commercially available dilution refrigerators and control systems.

The Novera QPU is available to order at rigetti.com/novera starting at $900,000 and ships within 4-6 weeks after the order is confirmed and shipping and logistics are finalized.

19.Post-quantum Cryptography (PQC): New Algorithms for a New Era

https://www.rambus.com/blogs/post-quantum-cryptography-pqc-new-algorithms-for-a-new-era/

Post-Quantum Cryptography (PQC), also known as Quantum Safe Cryptography (QSC), refers to cryptographic algorithms designed to withstand attacks by quantum computers.

Quantum computers will eventually become powerful enough to break public key-based cryptography, also known as asymmetric cryptography. Public key-based cryptography is used to protect everything from your online communications to your financial transactions.

Quantum computing represents a major security threat and action is needed now to secure applications and infrastructure using Post-Quantum/Quantum Safe Cryptography.

This blog explains everything you need to know about the new algorithms designed to protect against quantum computer attacks.

What is quantum computing?

Quantum computing utilizes quantum mechanics to solve certain classes of complex problems faster than is possible on classic computers. Problems that currently take the most powerful supercomputer several years could potentially be solved in days.

As such, quantum computers have the potential to deliver the computational power that could take applications like AI to a whole new level. Powerful quantum computers will become a reality in the not-so-distant future, and while they offer many benefits, they also present a major security threat.

Why are quantum computers a security threat?

Once sufficiently powerful quantum computers exist, traditional asymmetric cryptographic methods for key exchange and digital signatures will be broken. Leveraging Shor's algorithm, quantum computers will be capable of reducing the security of discrete logarithm-based schemes like Elliptic Curve Cryptography (ECC) and factorization-based schemes like RSA (Rivest-Shamir-Adleman) so much that no reasonable key size would suffice to keep data secure. ECC and RSA are the algorithms used to protect everything from our bank accounts to our medical records.

Governments, researchers, and tech leaders the world over have recognized this quantum threat and the difficulty in securing critical infrastructure against attacks from quantum computers.

"A quantum computer of sufficient size and sophistication — also known as a cryptanalytically relevant quantum computer (CRQC) — will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world.

When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."

What is Post-Quantum Cryptography (PQC)?

New digital signatures and key encapsulation mechanisms (KEMs) are needed to protect data and hardware from quantum attacks. Many initiatives have been launched throughout the world to develop and deploy new cryptographic algorithms that can replace RSA and ECC while being highly resistant to both classic and quantum attacks. Post-Quantum Cryptography (PQC) refers to these cryptographic algorithms designed to withstand attacks by quantum computers.

Is Quantum Safe Cryptography the same as Post-Quantum Cryptography (PQC)?

Yes, Quantum Safe Cryptography is another term for Post-Quantum Cryptography. Both refer to cryptographic algorithms designed to withstand attacks by quantum computers. Other terms that you may come across include Quantum Proof Cryptography or Quantum Resistant Cryptography.

Why do we need to act now if quantum computers are still a way off?

While quantum computers powerful enough to break public key encryption may still be a way off, data harvesting is happening now. Malicious actors are already said to be collecting encrypted data and storing it for the time when future quantum computers will be capable of breaking our current encryption methods. This is known as a "harvest now, decrypt later" strategy.

Further because the shelf life of confidential or private information can span years or decades, there is a rapidly growing need to protect such data today to future proof it from quantum attack. Additionally, for many devices such as chips, the development cycle is a long one. Given that it can take years for security testing, certification and then deployment into the existing infrastructure, the earlier the transition to Quantum Safe Cryptography begins, the better.

What progress has been made to develop new PQC algorithms?

The biggest public initiative to develop and standardize new PQC algorithms was launched by The U.S. Department of Commerce's National Institute of Standards and Technology (NIST). International teams of cryptographers submitted algorithm proposals, reviewed the proposals, broke some, and gained confidence in the security of others.

After multiple rounds of evaluations, on July 5th, 2022, NIST announced the first PQC algorithms selected for standardization. CRYSTALS-Kyber was selected as a Key Encapsulation Mechanism (KEM) and CRYSTALS-Dilithium, FALCON, and SPHINCS+ were selected as digital signature algorithms.

On August 24th, 2023, NIST announced the first three draft standards for general-purpose Quantum Safe Cryptography.

These are draft standards are:

- FIPS 203 ML-KEM: Module-Lattice-Based Key Encapsulation Mechanism Standard, which is based on the previously selected CRYSTALS-Kyber mechanism
- FIPS 204 ML-DSA: Module-Lattice-Based Digital Signature Standard, which is based on the previously selected CRYSTALS-Dilithium signature scheme
- FIPS 205 SLH-DSA: Stateless Hash-Based Digital Signature Standard, which is based on the previously selected SPHINCS+ signature scheme

What recommendations does CNSA 2.0 make for transitioning to PQC algorithms?

The National Security Agency (NSA) published an update to its Commercial National Security Algorithm Suite (CNSA) in September 2022, CNSA 2.0.

National Security Systems (NSS) will need to fully transition to PQC algorithms by 2033 and some use cases will be required to complete the transition as early as 2030. CNSA 2.0 specifies that CRYSTALS-Kyber and CRYSTALS-Dilithium should be used as quantum-resistant algorithms, along with stateful hash-based signature schemes XMSS (eXtended Merkle Signature Scheme) and LMS (Leighton-Micali Signatures).

CNSA 2.0 sets out an ambitious timeline for PQC algorithm adoption – other organizations across the globe are set to follow suit with their own guidelines.

How can companies get ready for the Quantum Computing Era?

- Understand where vulnerable cryptography like RSA or ECC is deployed in your products.
- Investigate what performance impact a PQC transition will have on your products and what makes sense for your product roadmap.

- Establish what transition timelines your products must observe.
- Speak with your customers and suppliers to ensure that expectations and plans align.
- Understand where vulnerable cryptography like RSA or ECC is deployed in your business infrastructure and business processes.
- Talk to security experts like Rambus to understand how you can begin to transition to Quantum Safe Cryptography

What Quantum Safe IP solutions are available from Rambus?

Rambus Quantum Safe IP solutions offer a hardware-level security solution to protect data and hardware against quantum computer attacks using NIST and CNSA selected algorithms.

Rambus Quantum Safe IP products are compliant with FIPS 203 ML-KEM and FIPS 204 ML-DSA draft standards. Products are firmware programmable to allow for updates with evolving quantum-resistant standards.

The products can be deployed in ASIC, SoC and FPGA implementations for a wide range of applications including data center, AI/ML, defense and other highly secure applications.

Solution	Applications
QSE-IP-86	Standalone engine providing Quantum Safe Cryptography acceleration
QSE-IP-86 DPA	Standalone engine providing Quantum Safe Cryptography acceleration and DPA-resistant cryptographic accelerators
RT-634	Programmable Root of Trust with Quantum Safe Cryptography acceleration
RT-654	Programmable Root of Trust with Quantum Safe Cryptography acceleration and DPA-resistant cryptographic accelerators
RT-664	Programmable Root of Trust with Quantum Safe Cryptography acceleration and FIA-protected cryptographic accelerators

Summary

Quantum computing is being pursued across industry, government and academia with tremendous energy and is set to become a reality in the not-so-distant future. For many years, Rambus has been a leading voice in the PQC movement and now offers a portfolio of Quantum Safe IP solutions designed to offer hardware-level security using NIST and CNSA selected algorithms.

20.The hardware and software for the era of quantum utility is here

by Jay Gambetta
https://research.ibm.com/blog/quantum-roadmap-2033

We've entered a new era of quantum computing.

We define eras using themes that unite periods of time. In the case of quantum computing, the theme of the past few decades has been the emergence and establishment of this new technology. The community focused on laying the groundwork: experimenting with quantum hardware, devising use cases, and educating people on how to use quantum computers, while running experiments benchmarking devices. We made quantum computing real.

But earlier this year, we published an experiment that changed the status quo. We demonstrated that quantum computers could run circuits beyond the reach of brute-force classical simulations. For the first time, we have hardware and software capable of executing quantum circuits with no known a priori answer at a scale of 100 qubits and 3,000 gates. Quantum is now a computational tool, and what makes me most excited is that we can start to advance science in fields beyond quantum computing, itself.

I like to say users are using quantum computing to do quantum computing, and we are adding capabilities that open up quantum to an extended set of users that includes what we refer to as quantum computational scientists. We think this is proof enough that we've entered a new era.

From these large-scale experiments, it has become clear that we must go beyond the traditional circuit model and take advantage of parallelism, concurrent classical computing, and dynamic circuits. We have ample evidence that, with tools such as circuit knitting, we can enhance the reach of quantum computation, and new quantum algorithms are emerging that make use of multiple quantum circuits, potentially in parallel and with concurrent classical operations. It is clear that a heterogeneous computing architecture consisting of scalable and parallel circuit execution and advanced classical computation is required.

This is our vision for the high-performance systems for the future: quantum-centric supercomputing. At this year's IBM Quantum Summit, we announce major updates that bring us closer to this goal, as well as an extended roadmap that details the journey toward quantum-centric supercomputing over the next decade — allowing more advanced utility-scale work and a frictionless development environment for our users.

Breaking the 1,000-qubit barrier with Condor

We have introduced **IBM Condor, a 1121 superconducting qubit quantum processor** based on our cross-resonance gate technology. Condor pushes the limits of scale and yield in chip design with a 50% increase in qubit density, advances in qubit fabrication and laminate size, and includes over a mile of high-density cryogenic flex IO wiring within a single dilution refigerator. With performance comparable to our previous **433-qubit Osprey**, it serves as an innovation milestone, solving scale and informing future hardware design.

Access to the highest performing quantum processor: Heron

Building on four years of research, we introduced **the first IBM Quantum Heron processor** on the ibm_torino quantum system. Featuring 133 fixed-frequency qubits with tunable couplers, Heron yields a 3-5x improvement in device performance over our previous **flagship 127-qubit Eagle processors**, and virtually eliminates cross-talk. With Heron, we have developed a qubit and the gate technology that we're confident will form the foundation of our hardware roadmap going forward.

IBM Quantum System Two: The system for a decade of scalable quantum computation

IBM Quantum System Two is the bedrock for scalable quantum computation, and is now operational at our lab in Yorktown Heights, NY. It is 22 feet wide, 12 feet high, and today features three IBM Quantum

Heron processors. It combines cryogenic infrastructure with third-generation control electronics and classical runtime servers.

IBM Quantum System Two is the modular-architecture quantum computing platform that we will use to realize parallel circuit executions for quantum-centric supercomputing.

Qiskit 1.0 coming in February 2024

Quantum-centric supercomputing is not achieved by hardware alone. It requires performant software for generating and manipulating quantum circuits and middleware for executing hybrid quantum-classical workflows in a heterogeneous computing environment. Qiskit 1.0 marks the first stable release of Qiskit, the most popular quantum computing SDK. It delivers marked improvements in circuit construction, compilation times, and memory consumption compared to earlier releases.

In addition, Qiskit 1.0 outperforms competing compilation frameworks in both runtime and resultant two-qubit gate counts when mapping circuits to quantum hardware.

AI transpilation alpha for Premium Users

IBM brings the power of AI to quantum computing with the world's first circuit compilation service using reinforcement learning running on the IBM Quantum Platform. This initial preview demonstrates a reduction in two-qubit gate count of 20-50% compared to standard heuristic methods.

Execution modes

To further optimize throughput when executing multiple independent jobs, we introduce batch mode — a new execution mode yielding up to a 5x improvement in execution time relative to single-job submission. In addition, for utility-scale iterative workloads we have released extended Sessions, which allow for combining multiple Sessions together to seamlessly enable advanced quantum-classical workloads.

Qiskit Patterns and Quantum Serverless

IBM introduced Qiskit Patterns, a programming template outlining the structure of quantum programs and a logical framework for building quantum algorithms and applications at scale. Taking advantage of the composability, containerization, and abstraction provided by Qiskit Patterns, users can seamlessly create quantum algorithms and applications from a collection of foundational building blocks and execute those Patterns using heterogeneous computing infrastructure such as Quantum Serverless. This allows for targeted quantum acceleration of preexisting enterprise scale workflows and provides for abstraction away from quantum circuits and operators. With Qiskit Patterns, IBM is announcing the deployment of Quantum Serverless as beta for managed, unattended execution of Patterns at scale.

Generative AI for quantum on watsonx

To better streamline the quantum development process, IBM is pioneering the use of generative AI for quantum code programming through watsonx, the enterprise AI platform from IBM. We demonstrate how generative AI available through watsonx can help automate the development of quantum code for Qiskit. We achieve this through the fine-tuning of the IBM Granite 20-billion parameter code foundation model.

Extended roadmap to 2033

In order to guide our mission to realize quantum-centric supercomputing, we are expanding our industry-defining roadmap out to 2033 for a decade worth of quantum innovation. The roadmap highlights improvements in the number of gates that our processors and systems will be able to execute. Starting

with a target of Heron reaching 5,000 gates in 2024, the roadmap lays out multiple generations of processors, each leveraging improvements in quality to achieve ever-larger gate counts.

Then, in 2029, we hit an inflection point: executing 100 million gates over 200 qubits with our Starling processor employing error correction based on the novel Gross code. This is followed by Blue Jay, a system capable of executing 1 billion gates across 2,000 qubits by 2033. This represents a nine order-of-magnitude increase in performed gates since we put our first device on the cloud in 2016. Our new innovation roadmap will demonstrate the technology needed to realize the Gross code through l-, m-, and c-couplers to be demonstrated by Flamingo, Crossbill, and Kookaburra processors, respectively.

Laying the groundwork for quantum-powered use cases

University of Tokyo, Argonne National Laboratory, Fundacion Ikerbasque, Qedma, Algorithmiq, University of Washington, University of Cologne, Harvard University, UC Berkeley, Q-CTRL all demonstrated new research to explore the power of utility-scale quantum computing. These demonstrations showed that advances in both device quality and new capabilities are allowing us to explore more challenging circuits, extending beyond quantum computing native problems to use quantum and classical working together to extend the reach of the systems.

Updating our offerings for the era of utility

Entering the era of utility means a shift of focus to providing a Qiskit Runtime service designed for utility-scale experiments and availability to utility-scale systems across all of our access plans. Now, we make 100+ qubit systems available on our Open Plan to provide free access to start your quantum journey, on our Pay-As-You-Go Plan, on our Premium Plan that provides reserved capacity, and on our Dedicated Service which provides a dedicated managed system deployed at our partners' locations.

Quantum Accelerator 3.0

Entering the era of utility opens up new opportunities for enterprises to engage with quantum computing and explore workforce integration. We are expanding our enterprise offerings to continue to advance industry use cases for utility-scale quantum computing.

IBM Quantum Safe

This progress in quantum technology also means that to keep our data secure, we need new cryptography based on mathematical problems that are challenging to both quantum and classical computers. IBM Quantum Safe helps enterprises assess their cryptographic posture and modernize their cybersecurity landscape for the era of quantum utility.

Our updated IBM Quantum Safe roadmap highlights how we are continuing to advance research into quantum-safe cryptography, foster industry partnerships to drive adoption of post-quantum cryptographic solutions, and develop new quantum-safe technologies — including IBM Quantum Safe Explorer, our cryptographic discovery tool released this past October.

21.Celebrated Cryptography Algorithm Gets an Upgrade

by Madison Goldberg

https://www.quantamagazine.org/celebrated-cryptography-algorithm-gets-an-upgrade-20231214/

Two researchers have improved a well-known technique for lattice basis reduction, opening up new avenues for practical experiments in cryptography and mathematics.

In our increasingly digital lives, security depends on cryptography. Send a private message or pay a bill online, and you're relying on algorithms designed to keep your data secret. Naturally, some people want to uncover those secrets — so researchers work to test the strength of these systems to make sure they won't crumble at the hands of a clever attacker.

One important tool in this work is the **LLL algorithm**, named after the researchers who published it in 1982 — **Arjen Lenstra, Hendrik Lenstra Jr. and László Lovász**. LLL, along with its many descendants, can break cryptographic schemes in some cases; studying how they behave helps researchers design systems that are less vulnerable to attack. And the algorithm's talents stretch beyond cryptography: It's also a useful tool in advanced mathematical arenas such as computational number theory.

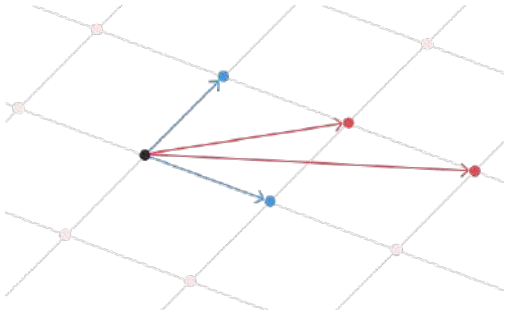
Over the years, researchers have honed variants of LLL to make the approach more practical — but only up to a point. Now, a pair of cryptographers have built a new LLL-style algorithm with a significant boost in efficiency. The new technique, which won the Best Paper award at the 2023 International Cryptology Conference, widens the range of scenarios in which computer scientists and mathematicians can feasibly use LLL-like approaches.

"It was really exciting," said Chris Peikert, a cryptographer at the University of Michigan who was not involved in the paper. The tool has been the focus of study for decades, he said. "It's always nice when a target that has been worked on for so long … shows that there's still surprises to be found."

LLL-type algorithms operate in the world of lattices: infinite collections of regularly spaced points. As one way of visualizing this, imagine you're tiling a floor. You could cover it in square tiles, and the corners of those tiles would make up one lattice. Alternatively, you could choose a different tile shape — say, a long parallelogram — to create a different lattice.

A lattice can be described using its "basis." This is a set of vectors (essentially, lists of numbers) that you can combine in different ways to get every point in the lattice. Let's imagine a lattice with a basis consisting of two vectors: [3, 2] and [1, 4]. The lattice is just all the points you can reach by adding and subtracting copies of those vectors.

That pair of vectors isn't the lattice's only basis. Every lattice with at least two dimensions has infinitely many possible bases. But not all bases are created equal. A basis whose vectors are shorter and closer to right angles with one another is usually easier to work with and more useful for solving some computational problems, so researchers call those bases "good." An example of this is the pair of blue vectors in the figure below. Bases consisting of longer and less orthogonal vectors — like the red vectors — can be considered "bad."



This is a job for LLL: Give it (or its brethren) a basis of a multi-dimensional lattice, and it'll spit out a better one. This process is known as lattice basis reduction.

What does this all have to do with cryptography? It turns out that the task of breaking a cryptographic system can, in some cases, be recast as another problem: finding a relatively short vector in a lattice. And sometimes, that vector can be plucked from the reduced basis generated by an LLL-style algorithm. This strategy has helped researchers topple systems that, on the surface, appear to have little to do with lattices.

In a theoretical sense, the original LLL algorithm runs quickly: The time it takes to run doesn't scale exponentially with the size of the input — that is, the dimension of the lattice and the size (in bits) of the numbers in the basis vectors. But it does increase as a polynomial function, and "if you actually want to do it, polynomial time is not always so feasible," said Léo Ducas, a cryptographer at the national research institute CWI in the Netherlands.

In practice, this means that the original LLL algorithm can't handle inputs that are too large. "Mathematicians and cryptographers wanted the ability to do more," said Keegan Ryan, a doctoral student at the University of California, San Diego. Researchers worked to optimize LLL-style algorithms to accommodate bigger inputs, often achieving good performance. Still, some tasks have remained stubbornly out of reach.

The new paper, authored by Ryan and his adviser, Nadia Heninger, combines multiple strategies to improve the efficiency of its LLL-style algorithm. For one thing, the technique uses a recursive structure that breaks the task down into smaller chunks. For another, the algorithm carefully manages the precision of the numbers involved, finding a balance between speed and a correct result. The new work makes it feasible for researchers to reduce the bases of lattices with thousands of dimensions.

Past work has followed a similar approach: A 2021 paper also combines recursion and precision management to make quick work of large lattices, but it worked only for specific kinds of lattices, and not all the ones that are important in cryptography. The new algorithm behaves well on a much broader range. "I'm really happy someone did it," said Thomas Espitau, a cryptography researcher at the company PQShield and an author of the 2021 version. His team's work offered a "proof of concept," he said; the new result shows that "you can do very fast lattice reduction in a sound way."

The new technique has already started to prove useful. Aurel Page, a mathematician with the French national research institute Inria, said that he and his team have put an adaptation of the algorithm to work on some computational number theory tasks.

LLL-style algorithms can also play a role in research related to lattice-based cryptography systems designed to remain secure even in a future with powerful quantum computers. They don't pose a threat to such systems, since taking them down requires finding shorter vectors than these algorithms can achieve. But the best attacks researchers know of use an LLL-style algorithm as a "basic building block," said Wessel van Woerden, a cryptographer at the University of Bordeaux. In practical experiments to study these attacks, that building block can slow everything down. Using the new tool, researchers may be able to expand the range of experiments they can run on the attack algorithms, offering a clearer picture of how they perform.

22.Telstra takes a step closer to quantum secure networking

https://www.idquantique.com/telstra-takes-a-step-closer-to-quantum-secure-networking/?utm_term=Find%20out%20more&utm_campaign=Quantum%20Era%20Security%20Times%3A%20December%202023&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%3A%20December%202023-_-Find%20out%20more

In October 2023, Corning published a whitepaper detailing the results of an experiment conducted at networking company Ciena Corporation's test labs in Ottawa, Canada. The experiment was designed to demonstrate performance improvements in quantum encryption, utilising Ciena's Waveserver® platform and IDQ's Cerberis XG QKD system, across Corning's ultra-low-loss fibre infrastructure.

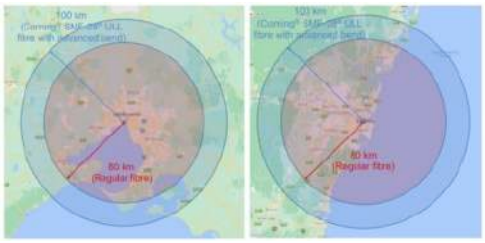
The benefits of QKD are well established. With adoption projected to grow exponentially over the coming years, there is evidence of a global initiative to address the challenges associated with wide area quantum networks. The fragile nature of quantum signals necessitates the use of trusted nodes if the network is to span great distances. While the use of trusted nodes can add cost and complexity to the network infrastructure, utilising ultra-low attenuation fibre can help extend the reach of the quantum signal, reducing the number of trusted nodes required.

The paper: Telstra InfraCo Advanced Fibre Technology Enhances QKD Encryption Performance considers two alternative QKD scenarios: intra-city and inter-city.

- The intra-city use case is confined to a single metro area, where distances are typically less than 100 km. This reflects what is known as single-hop transmission, where there is no need for trusted nodes to extend the quantum range.
- The inter-city use case explores a scenario where quantum communications are secured between geographically remote locations.

For illustration purposes, the experiment used Melbourne and Sydney as prospect sites.

In scenario one, the new low-attenuation fibre was compared to a typical G.652.D compliant NDS fibre, commonly in use around the world. The results were impressive, with a 25% increase in reach from 80 km to 100 km. The implications are significant, as the increase in reach represents an increase in target area for a second data centre by over 50%. The experiment also compared the secure key rate of the two fibre options over an identical distance (80 km). The new low-attenuation fibre significantly outperformed the legacy infrastructure, increasing the capacity to deliver QKD-grade security by 71%.



"An increase in distance by 25% corresponds to the additional area coverage of around 56% for the second data centre placement"

Fibre Type	Max Attenuation at 1550nm	Distance	SKR
NDSF	0.20	80km	1231
SMF-28 ULL	0.16	100km	1153

In scenario 2, this improved reach was used to illustrate significant potential savings for a network extending 900 km between the two orirginal sites in Melbourne and Sydney. The extended reach allows for the removal of 3 trusted nodes (from 11 to 8) between the two sites.

23.IBM Debuts Next-Generation Quantum

Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility

by Erin Angelini and Hugh Collins
https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility

Today (04 Dec 2023), at the annual IBM Quantum Summit in New York, IBM debuted 'IBM Quantum Heron,' the first in a new series of utility-scale quantum processors with an architecture engineered over the past four years to deliver IBM's highest performance metrics and lowest error rates of any IBM Quantum processor to date.

IBM also unveiled IBM Quantum System Two, the company's first modular quantum computer and cornerstone of IBM's quantum-centric supercomputing architecture. The first IBM Quantum System Two, located in Yorktown Heights, New York, has begun operations with three IBM Heron processors and supporting control electronics.

With this critical foundation now in place, along with other breakthroughs in quantum hardware, theory, and software, the company is extending its IBM Quantum Development Roadmap to 2033 with new targets to significantly advance the quality of gate operations. Doing so would increase the size of quantum circuits able to be run and help to realize the full potential of quantum computing at scale.

"We are firmly within the era in which quantum computers are being used as a tool to explore new frontiers of science," said Dario Gil, IBM SVP and Director of Research. "As we continue to advance how quantum systems can scale and deliver value through modular architectures, we will further increase the quality of a utility-scale quantum technology stack – and put it into the hands of our users and partners who will push the boundaries of more complex problems."

As demonstrated by IBM earlier this year on a 127-qubit '**IBM Quantum Eagle**' processor, IBM Quantum systems can now serve as a scientific tool to explore utility-scale classes of problems in chemistry, physics, and materials beyond brute force classical simulation of quantum mechanics.

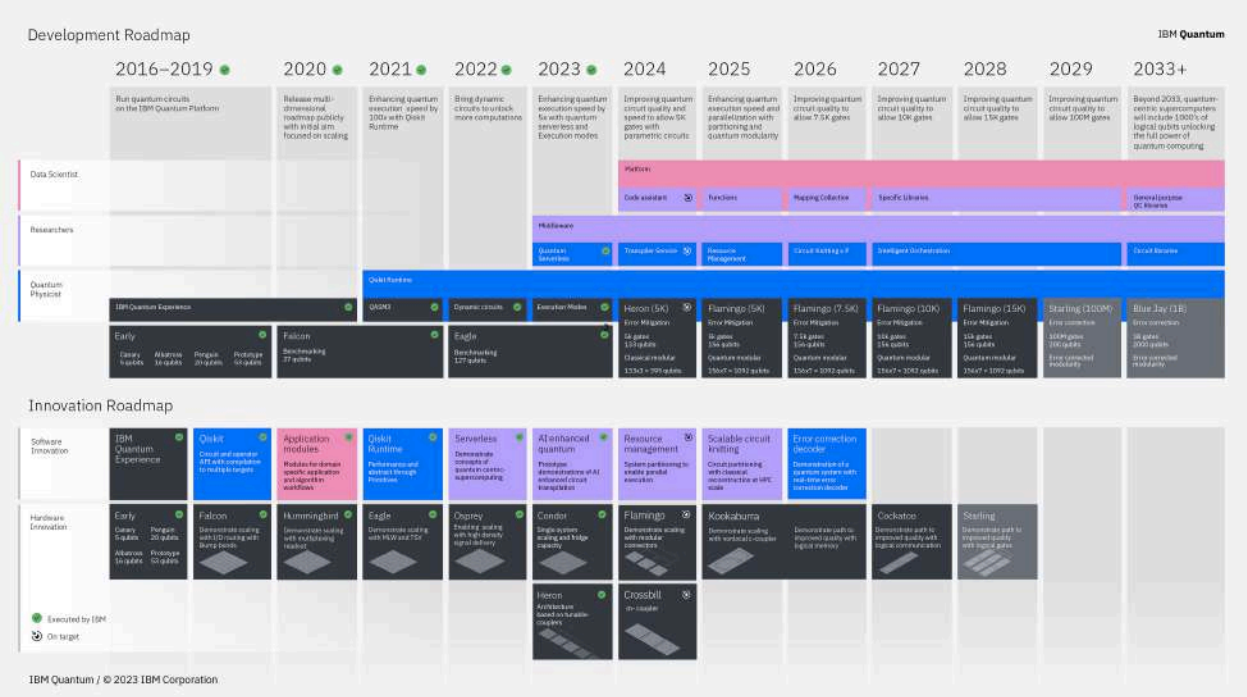
Since that demonstration, leading researchers, scientists, and engineers from organizations including the U.S. Department of Energy's Argonne National Laboratory, the University of Tokyo, the University of Washington, the University of Cologne, Harvard University, Qedma, Algorithmiq, UC Berkeley, Q-CTRL, Fundacion Ikerbasque, Donostia International Physics Center, and the University of the Basque Country, as well as IBM, have expanded demonstrations of utility-scale quantum computing to confirm its value in exploring uncharted computational territory.

This includes experiments already running on the **new IBM Quantum Heron 133-qubit processor**, which IBM is making available for users today via the cloud. IBM Heron is the first in IBM's new class of performant processors with significantly improved error rates, offering a five-times improvement over the previous best records set by IBM Eagle. Additional IBM Heron processors will join IBM's industry-leading, utility-scale fleet of systems over the course of the next year.

IBM Quantum System Two and Extended IBM Quantum Development Roadmap

IBM Quantum System Two is the foundation of IBM's next generation quantum computing system architecture. It combines scalable cryogenic infrastructure and classical runtime servers with modular qubit control electronics. The new system is a building block for IBM's vision of quantum-centric supercomputing. This architecture combines quantum communication and computation, assisted by classical computing resources, and leverages a middleware layer to appropriately integrate quantum and classical workflows.

As part of the newly expanded ten-year IBM Quantum Development Roadmap, IBM plans for this system to also house IBM's future generations of quantum processors. Also, as part of this roadmap, these future processors are intended to gradually improve the quality of operations they can run to significantly extend the complexity and size of workloads they are capable of handling.



Qiskit and Generative AI to Increase Ease of Quantum Software Programming

Today, IBM is also detailing plans for a new generation of its software stack, within which Qiskit 1.0 will be a pivot point defined by stability and speed. Additionally, and with the goal of democratizing quantum computing development, IBM is announcing Qiskit Patterns.

Qiskit Patterns will serve as a mechanism to allow quantum developers to more easily create code. It is based in a collection of tools to simply map classical problems, optimize them to quantum circuits using Qiskit, executing those circuits using Qiskit Runtime, and then postprocess the results. With Qiskit Patterns, combined with Quantum Serverless, users will be able to build, deploy, and execute workflows integrating classical and quantum computation in different environments, such as cloud or on-prem scenarios. All of these tools will provide building blocks for users to build and run quantum algorithms more easily.

Additionally, IBM is pioneering the use of generative AI for quantum code programming through watsonx, IBM's enterprise AI platform. IBM will integrate generative AI available through watsonx to help automate the development of quantum code for Qiskit. This will be achieved through the finetuning of the IBM Granite model series.

"Generative AI and quantum computing are both reaching an inflection point, presenting us with the opportunity to use the trusted foundation model framework of watsonx to simplify how quantum algorithms can be built for utility-scale exploration," said Jay Gambetta, Vice President and IBM Fellow at IBM. "This is a significant step towards broadening how quantum computing can be accessed and put in the hands of users as an instrument for scientific exploration."

With advanced hardware across IBM's global fleet of 100+ qubit systems, as well as easy-to-use software that IBM is debuting in Qiskit, users and computational scientists can now obtain reliable results from quantum systems as they map increasingly larger and more complex problems to quantum circuits.

24.U.K. Advances National Quantum Strategy Through Quantum Missions

by Robert Huntley
https://www.eetimes.eu/u-k-advances-national-quantum-strategy-through-quantum-missions/

2023 was a busy year for quantum technology in the U.K. In March, The Rt. Hon. Michelle Donelan MP, Secretary of State for Science, Innovation and Technology, launched the U.K. Quantum Strategy that promised £2.5 billion (€2.9 billion) of government funding over the next decade. This announcement built on the 2014 program to invest £1 billion (~€1.1 billion) in quantum research and development and establish national quantum technology hubs. Recently, the U.K. Quantum Showcase, an annual indicator of the U.K.'s quantum scene, highlighted a flurry of R&D activity and an active investment environment.

In this year's Autumn Statement, The Rt. Hon. Jeremy Hunt, Chancellor of the Exchequer, added more color to the U.K.'s Quantum Strategy with the announcement of five quantum missions to give focus and direction to quantum technology research and development efforts. The missions include timelines for specific outcomes, and at least two of the five highlight the need for early commercialization.

U.K. quantum missions

Mission 1 stipulated that by 2035, there will be accessible U.K.-based quantum computers capable of running at 1 trillion operations per second and that applications running on them should provide operational benefits more significant than those provided by classical computers across critical sectors of the U.K. economy.

Mission 2, with a goal of deploying the world's most advanced quantum network at scale by 2035, might be more of a challenge, especially as other nation-states may wish to claim the same outcome.

The benefits that quantum sensing technologies may deliver to healthcare and help those with chronic illness are identified in **Mission 3**, with the goal that by 2030, every U.K. National Health Service (NHS) Trust will benefit.

The increasing threats posed by GNSS vulnerabilities to positioning, navigation and timing (PNT) applications have shaped **Mission 4**. Developing highly accurate quantum clocks small enough to incorporate into mobile devices will form part of the recently announced U.K. PNT policy framework, with a 2030 timeline.

Mission 5 is a catch-all and broad-reaching initiative. With the goal that by 2030, mobile and networked

quantum sensors will have unlocked new situational-awareness capabilities, it highlights the need to accelerate the development of quantum technologies and catalyze the private investment necessary to take innovations through to commercial adoption.

Commercialization key

The U.K. Quantum Strategy and quantum missions are good news for the U.K. scientific and technology community and, with the promised funding, will no doubt result in many exciting quantum technologies. However, the ultimate success of these quantum innovations depends on the ability to get them adopted. Historically, the U.K. needs to improve technology commercialization. Obtaining funding to get innovations out of the lab and into the market is often quoted as a significant stumbling block. Also, since Brexit, the U.K. might appear to be taking a parochial stance rather than embracing a more internationally facing approach.

To learn how the U.K. quantum community has received the launch of the quantum missions, EE Times Europe interviewed three U.K. quantum innovators: Ashley Montanaro, CEO and co-founder of Phasecraft; Ben Packman, senior vice president of strategy at PQShield; and Chris Ballance, CEO of Oxford Ionics.

Quantum algorithms and software as crucial as quantum hardware

Quantum algorithms company Phasecraft (Bristol and London, U.K.) develops algorithms that reduce the error rate of quantum computers. Reducing errors is essential for any quantum hardware to scale to achieve significant computational throughput.

“It’s fantastic to see the government investing in these missions, and in fact, we were involved in helping to shape them,” Montanaro said. “What is critically important is that the government has also recognized that algorithms and software are just as important as the development of quantum hardware. Also, they see that it is crucial to support algorithm development in the near and long terms. The government understands that realizing the full potential of quantum computing is a marathon, not a sprint. It is really going to help make the U.K. one of the best places in the world to work in quantum.”

In August 2023, Phasecraft closed a £13 million (€15 million) Series A funding round. Montanaro told EE Times Europe the company also won U.K. government funding for two quantum algorithm R&D projects: One is researching and selecting clean energy materials, and the other is solving complex optimization problems relevant to energy grids.

“We’re trying to get the most out of near-term quantum computers, which exist now or [will exist] in the next few years,” Montanaro said. “These machines are somewhat limited in terms of their size. However, they can solve problems that classical computers struggle to solve today but are still relativity limited compared with quantum computers of the far future.”

Montanaro likened today’s quantum computers to the development of classical computers in the 1940s and 1950s. He said the biggest challenge is solving complex problems on limited quantum platforms, and hence the need for ultra-efficient algorithms.

Talent availability is an industry-wide problem

When asked about the broad challenges they face as a business, Montanaro said, “The availability of talent is a real bottleneck for the whole industry because quantum computing is a very specialized field. Most staff on Phasecraft’s R&D team have Ph.D.s on this topic, but more of these people are required. As a business, we can help mitigate this shortage. For example, we’re working with Ph.D. students at universities and have an internship program, and we also try to make sure we’re doing exciting work so people are highly motivated to come and join us. However, it is still a challenge the whole quantum in-

dustry is facing."

Another challenge appears that there has been a degree of nervousness among some governments in terms of the security and export control aspects associated with quantum technologies. One part concerns the cryptographic abilities that quantum computers can unleash against classical encryption and signature algorithms.

There also appears to be a hardening of international cooperation, which Montanaro believes may restrict development: "As an industry, we need to collaborate and work with partners in different countries and hire the top people wherever they are in the world. We think quantum computing should be an international technology."

Quantum missions lack security emphasis

PQShield's Packman told EE Times Europe, "As quantum computing and research accelerates, the need for quantum-safe cryptography becomes more acute and more urgent, so we're intrinsically tied to the quantum missions even though we're not developing quantum technology. From our perspective, we're somewhat disappointed that they don't tackle the security element at all. That's a bit of an omission and one that should probably be corrected in some way."

Packman observed that for the U.K. government's goal to build an advanced quantum network at scale (Mission 2), it should first adopt post-quantum cryptography (PQC). By so doing, as it scales, it will be secure, and the computational capabilities will be ready to aid markets like healthcare. He pointed out that the U.K.'s NHS is one of the largest healthcare systems in the world, and driving the quantum agenda into healthcare without it being quantum-secure didn't make sense.

Post-quantum cryptography

PQC company PQShield (Oxford, U.K.) is at the forefront of defining PQC algorithms and recently hosted an international event in Oxford to review the PQC standards proposed by NIST. EE Times Europe asked Packman what progress had been like since the Oxford Summit. "That work is now concluding, and the standards are on track to be finalized early next year," he said. "That puts the process of defining the new NIST PQC algorithms to bed, but there's now a flow-down that needs to happen across the other standards bodies. People now need to go from being aware to actively planning. There'll be a demand for understanding exactly how these algorithms work in software and hardware, then moving on to system design."

Packman pointed out the massive challenge of getting the standards sorted and that their efforts of gathering world experts in cryptography at the Oxford conference significantly eased the technical difficulties involved. "Every line of code we write, every mathematical problem we solve, every interaction we make is all focused on keeping us one step ahead of the attackers," he said.

Establishing bridgehead markets

Oxford Ionics (Kidlington, U.K.) has developed a patented electronic qubit control (EQC) system to control qubits inside trapped-ion quantum processors. These processors initially used lasers to control qubits, but this approach does not scale, becoming increasingly error-prone as the number of qubits increases. With EQC, Oxford Ionics can harness the unrivaled quantum performance of individual atoms with the scalability and reliability of semiconductor ICs. The company announced a £30 million (~€35 million) Series A funding round in January 2023.

EE Times Europe asked CEO Ballance what the missions mean for the company. "The U.K. has done really well in the past, creating a hotbed of innovation of new technologies," he said. "However, when companies formed from these developments, they went to the U.S. for capital. For me, the missions are

a clear signal from the U.K. government that we're not going to let that happen again and will try to catalyze and grow the quantum technologies in the U.K."

Ballance noted they are well-aligned with the mission to build useful quantum computers and that its EQC technology reduces errors, an essential requirement to scale quantum computers. When asked what markets they aim to address, Ballance told EE Times Europe, "You need to know which direction you are going in. A few hundred qubits can be useful, but you need a few thousand low-error qubits to tackle big problems. For us, it's all about finding those bridgehead markets and endlessly pursuing those and all other distractions."

Ballance defined a bridgehead market as one that is limited on compute and where small advances in computational capability make a big difference to the bottom line: "This is broadly the financial markets, where people pay a lot of money for a slight edge and have relatively long-time horizons to invest in. Second, iterating materials is incredibly expensive, so any computational tools that help you learn faster massively decrease your time to market."

Talent acquisition and growth capital priorities

EE Times Europe asked Ballance if they had problems finding suitable talent, He said, "Any growth company is going to spend time thinking about talent acquisition, but at the moment, it's not a bottleneck for our growth. However, if we could wave a magic wand, the two things we'd want to improve are talent acquisition and growth capital. But that's the sign of a healthy company, I think. Also, it's a very international market at the moment, and we have teams worldwide."

Asked if he felt the U.K. Quantum initiatives might be too U.K.-focused, Ballance said, "We are a worldwide company and we operate worldwide. There is a strong geopolitical angle from the U.K. government and governments in general as to where the quantum computing industry will settle. Where's the Silicon Valley of quantum going to be? Where's the TSMC of quantum going to be?"

Ballance noted that the quantum industry is quite mobile now but that the next three to five years will be critical for where the industry settles and clustering begins: "The U.K. has got a really good head start because of the quantum technology hubs started 10 years ago. About half of my team came from those hubs."

Looking to the next five years, Ballance said, "Making sure the supply chain develops and talent stays in the right place and grows will be the next set of challenges."

25.A Physicist Reveals the One Quantum Breakthrough That Could Disrupt Scientific Innovation

by Daniel Lidar
https://www.inverse.com/science/physicist-reveals-quantum-breakthrough-disrupt-scientific-innovation

Quantum advantage is the milestone the field of quantum computing is fervently working toward, where a quantum computer can solve problems that are beyond the reach of the most powerful non-quantum or classical computers.

Quantum refers to the scale of atoms and molecules where the laws of physics as we experience them break down, and a different, counterintuitive set of laws apply. Quantum computers take advantage of these strange behaviors to solve problems.

There are some types of problems that are impractical for classical computers to solve, such as cracking state-of-the-art encryption algorithms. Research in recent decades has shown that quantum computers have the potential to solve some of these problems. If a quantum computer can be built that actually does solve one of these problems, it will have demonstrated quantum advantage.

I am a physicist who studies quantum information processing and the control of quantum systems. I believe that this frontier of scientific and technological innovation not only promises groundbreaking advances in computation but also represents a broader surge in quantum technology, including significant advancements in quantum cryptography and quantum sensing.

APPLICATIONS OF QUANTUM COMPUTING

Quantum computing has a range of potential uses where it can outperform classical computers. In cryptography, quantum computers pose both an opportunity and a challenge. Most famously, they have the potential to decipher current encryption algorithms, such as the widely used RSA scheme.

One consequence of this is that today's encryption protocols need to be re-engineered to be resistant to future quantum attacks. This recognition has led to the burgeoning field of post-quantum cryptography. After a long process, the National Institute of Standards and Technology recently selected four quantum-resistant algorithms and has begun the process of readying them so that organizations around the world can use them in their encryption technology.

In addition, quantum computing can dramatically speed up quantum simulation: the ability to predict the outcome of experiments operating in the quantum realm. Famed physicist Richard Feynman envisioned this possibility more than 40 years ago. Quantum simulation offers the potential for considerable advancements in chemistry and materials science, aiding in areas such as the intricate modeling of molecular structures for drug discovery and enabling the discovery or creation of materials with novel properties.

Another use of quantum information technology is quantum sensing: detecting and measuring physical properties like electromagnetic energy, gravity, pressure, and temperature with greater sensitivity and precision than non-quantum instruments. Quantum sensing has myriad applications in fields such as environmental monitoring, geological exploration, medical imaging, and surveillance.

Initiatives such as the development of a quantum internet that interconnects quantum computers are crucial steps toward bridging the quantum and classical computing worlds. This network could be secured using quantum cryptographic protocols such as quantum key distribution, which enables ultra-secure communication channels that are protected against computational attacks – including those using quantum computers.

Despite a growing application suite for quantum computing, developing new algorithms that make full use of the quantum advantage – in particular in machine learning – remains a critical area of ongoing research.

STAYING COHERENT AND OVERCOMING ERRORS

The quantum computing field faces significant hurdles in hardware and software development. Quantum computers are highly sensitive to any unintentional interactions with their environments. This leads to the phenomenon of decoherence, where qubits rapidly degrade to the 0 or 1 states of classical bits.

Building large-scale quantum computing systems capable of delivering on the promise of quantum speed-ups requires overcoming decoherence. The key is developing effective methods of suppressing and correcting quantum errors, an area my own research is focused on.

In navigating these challenges, numerous quantum hardware and software startups have emerged alongside well-established technology industry players like Google and IBM. This industry interest, combined with significant investment from governments worldwide, underscores a collective recognition of quantum technology's transformative potential. These initiatives foster a rich ecosystem where academia and industry collaborate, accelerating progress in the field.

QUANTUM ADVANTAGE COMING INTO VIEW

Quantum computing may one day be as disruptive as the arrival of generative AI. Currently, the development of quantum computing technology is at a crucial juncture. On the one hand, the field has already shown early signs of having achieved a narrowly specialized quantum advantage. Researchers at Google and later a team of researchers in China demonstrated a quantum advantage for generating a list of random numbers with certain properties. My research team demonstrated a quantum speed-up for a random number guessing game.

On the other hand, there is a tangible risk of entering a "quantum winter," a period of reduced investment if practical results fail to materialize in the near term.

While the technology industry is working to deliver quantum advantage in products and services in the near term, academic research remains focused on investigating the fundamental principles underpinning this new science and technology. This ongoing basic research, fueled by enthusiastic cadres of new and bright students of the type I encounter almost every day, ensures that the field will continue to progress.

26.Top 9 Cybersecurity Trends in 2024

by Linda Rosencrance
https://www.techopedia.com/cybersecurity-trends

With 2024 on the horizon, organizations must ensure that they prepare for the new and recurring cyberthreats that aim to bring them to their knees. Here are the top eight cybersecurity in 2024 from industry experts.

In recent years, businesses have increased their cybersecurity spending and enhanced security measures to stay ahead of cybercriminals.

However, threat actors have also improved their techniques, making it a never-ending battle between those aiming to protect their data and those trying to steal it.

As the New Year arrives, organizations must prepare for the new and recurring cyber threats that aim to bring them to their knees.

Here are the top nine cybersecurity trends in 2024 from industry experts.

Top 9 Cybersecurity Trends in 2024

9. Ransomware Continues to Be the Number One Threat as Gangs Go Global

8. Shift in the Dynamic Between CISOs and CIOs

7. The Impact of AI/GenAI on Cybersecurity

6. Increased Use of Info Stealer Malware to Carry Out Attacks

5. Compliance and Regulations Will Shake Up the Cybersphere

4. Small and Midsize Businesses Will Continue to Implement Emerging Tech

3. Quantum Computing Will Change the Cybersecurity Game

2. Collaboration Between DevOps and DevSecOps Increases

1. CISOs Will Develop/Refine Their Soft Skills

The Bottom Line

As the new year approaches, cybersecurity will continue to be a crucial issue for organizations because of the ever-increasing threat of cyberattacks.

As such, companies must prepare to meet these threats head-on and ensure that their sensitive corporate information is protected from cybercriminals.

