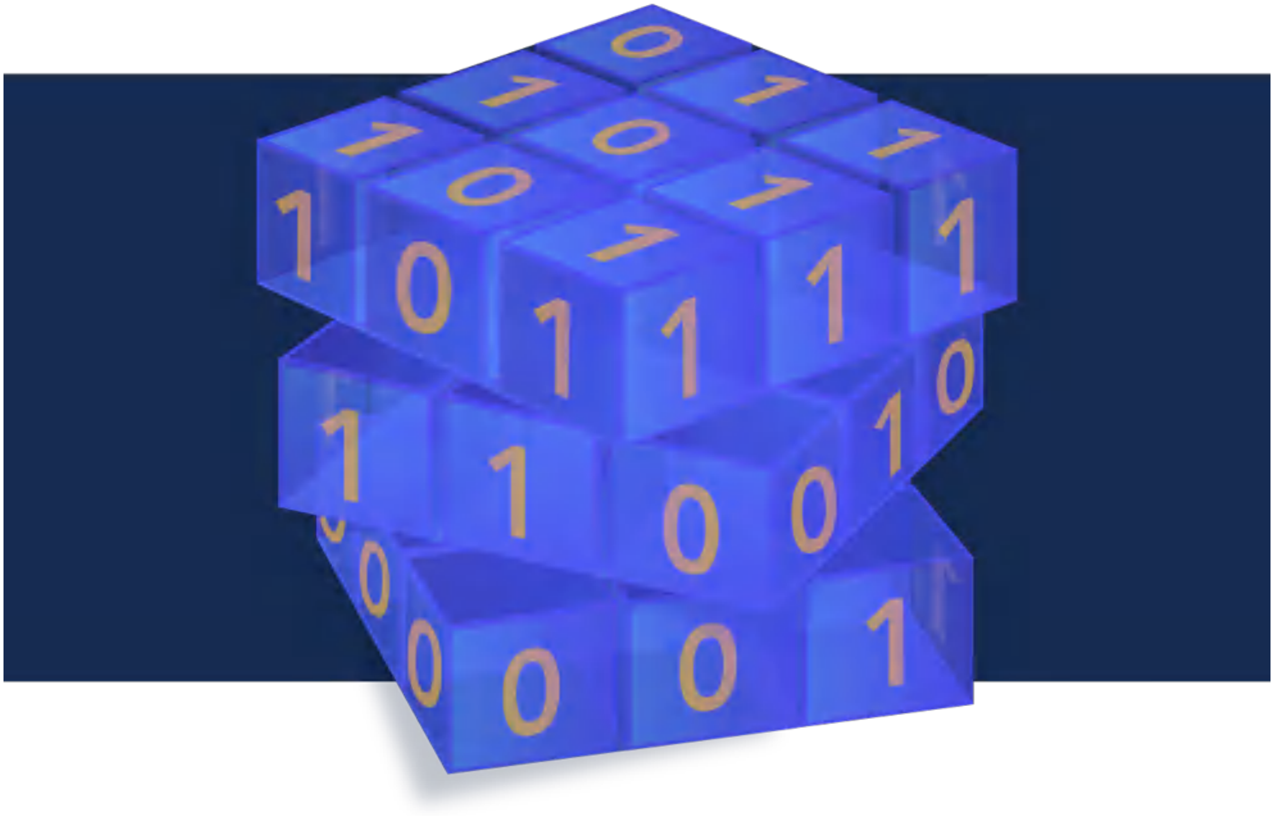
Crypto News

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

February 01, 2023



TABLES OF CONTENTS

Editorial

Happy February! Let's dive right in and change it up this month by starting with an article in the middle of our newsletter. If you're in Cybersecurity leadership you're going to want to read it. With the upcoming recession and tighter Cybersecurity budgets, how are you going to properly protect your organization from attackers? Go to article 20 to gain insight from industry experts about their Cybersecurity predictions for 2023 as well as their recommendations for success.

Next, you'll want to scroll to the end of the newsletter to article 29 which reports alarming news in the world of quantum computing. China claims that they have figured out how to break RSA public-key encryption using a quantum computer. However, industry experts, including yours truly, are skeptical. The paper released is not peer reviewed and the researchers do not have access to a quantum computer with nearly enough qubits to prove their theory. It seems for now that we have averted this crisis, but breaking RSA encryption as well as other alarming side-effects of quantum computing are inevitable. This is why you'll want to prepare now for a post-quantum world. Articles 8 and 19 are perfect examples of industry experts warning governments and organizations alike to act on quantum computing before it's too late. Are you and your organization going to heed this warning or will you act when it's already too late?

Make sure to take some time and read the other exciting articles in this edition of CryptoNews! I promise, you're going to "love" them (was that a subtle enough Valentine's Day reference?)!

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

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

1.Chinese Scientists Make Quantum Leap With First Practical Use Computer

by Zhang Tong
https://www.scmp.com/news/china/science/article/3208568/chinese-scientists-make-quantum-leap-first-practical-use-computer

China has become the third country – after Canada and the US – capable of delivering a complete computer system using game changing quantum technology, according to a state media report on Monday.

The country's first practical quantum computer – the 24-qubit Wuyuan, based on superconducting chip technology – was delivered to an unnamed user more than a year ago, the science ministry's newspaper Science and Technology Daily said.

It was the first official confirmation that this disruptive technology – which uses elemental particles called qubits to replace the 0 and 1 used in traditional computing – has been used in a real-life application in China. No details were given of the user or the computer's potential applications.

The report said Origin Quantum, a company founded in 2017 by Guo Guoping and Guo Guangcan – leading quantum physicists with the University of Science and Technology of China (USTC) – had developed several computers since delivering the Wuyuan in 2021.

The unparalleled computing power of quantum technology is expected to transform many areas, but its numerous technical challenges have led some scientists to believe that a practical machine is still years, if not decades away.

Previous quantum processors – Google's Sycamore and the photonic quantum computer Jiuzhang, built by Pan Jianwei at the USTC in Hefei, Anhui province – have proven their ability to surpass classical computers in solving specific mathematical questions.

But, they have not directly corresponded to any problems arising in actual production or life situations.

n an interview published by Shanghai-based news website The Paper on Monday, Origin Quantum co-founder Guo Guoping said the technology would produce visible benefits in daily life within the next three to five years.

"Quantum computers can act as accelerators. For example, a problem might take 10 traditional supercomputers a month to calculate. If a quantum computer is added to the computing group, the calculation time may be reduced to three to seven days," he said.

Quantum computers also have intrinsic advantages in the development of new materials and medicines, which are built using the atomic-scale calculations described by quantum mechanics.

"Using the tools that follow quantum mechanics to study the quantum world is more efficient than traditional computers," Guo said.

The company's quantum computers were built using two very different technical routes, he told The Paper. The superconducting version can more easily use quantum phenomena, such as superposition and entanglement, but needs to operate in extremely cold temperatures.

In contrast, semiconductor quantum computers share the same chip technology used in classical computing and the equipment and skills needed are also highly consistent. “But scientifically speaking, nobody knows which path is the right one,” he said.

Over the past 20 years, Guo has witnessed the birth and development of China's quantum technology. When he was a graduate student, the field of semiconductor quantum computing in China was a blank slate, he said.

Today, Chinese quantum computing has moved beyond purely scientific research to a stage where engineering technology is also emphasised, Guo said.

For its Wuyuan computer, Origin Quantum established a quantum ecological chain with an operating system, software and a computing cloud platform. The company also developed a range of superconducting quantum chips.

A more powerful quantum computer, named Wukong after the legendary Monkey King, will be available “soon”, according to Guo.

Despite the dawn of quantum computing products and applications, the company has yet to make a profit. In an interview last year with China Science Daily, Guo said the cost of research – 100 to 200 million yuan (US$14.8 to US$29.6 million) per year – meant Origin Quantum was living beyond its means.

“The company may not be profitable for the next 10 years,” he said.

But the goal is clear: to develop an engineered quantum computer that can be used interactively by users, so that China has independent and controllable quantum computing capabilities.

2.RSA's Demise From Quantum Attacks Is Very Much Exaggerated, Expert Says

by Dan Goodin
https://arstechnica.com/information-technology/2023/01/fear-not-rsa-encryption-wont-fall-to-quantum-computing-anytime-soon/

Three weeks ago, panic swept across some corners of the security world after researchers discovered a breakthrough that, at long last, put the cracking of the widely used RSA encryption scheme within reach by using quantum computing.

Scientists and cryptographers have known for two decades that a factorization method known as Shor's algorithm makes it theoretically possible for a quantum computer with sufficient resources to break RSA. That's because the secret prime numbers that underpin the security of an RSA key are easy to calculate using Shor's algorithm. Computing the same primes using classical computing takes billions of years.

The only thing holding back this doomsday scenario is the massive amount of computing resources required for Shor's algorithm to break RSA keys of sufficient size. The current estimate is that breaking a 1,024-bit or 2,048-bit RSA key requires a quantum computer with vast resources. Specifically, those resources are about 20 million qubits and about eight hours of them running in superposition. (A qubit is a basic unit of quantum computing, analogous to the binary bit in classical computing. But whereas a classic binary bit can represent only a single binary value such as a 0 or 1, a qubit is represented by a superposition of multiple possible states.)

The paper, published three weeks ago by a team of researchers in China, reported finding a factorization method that could break a 2,048-bit RSA key using a quantum system with just 372 qubits when it operated using thousands of operation steps. The finding, if true, would have meant that the fall of RSA encryption to quantum computing could come much sooner than most people believed.

RSA's demise is greatly exaggerated

At the Enigma 2023 Conference in Santa Clara, California, on Tuesday, computer scientist and security and privacy expert Simson Garfinkel assured researchers that the demise of RSA was greatly exaggerated. For the time being, he said, quantum computing has few, if any, practical applications.

"In the near term, quantum computers are good for one thing, and that is getting papers published in prestigious journals," Garfinkel, co-author with Chris Hoofnagle of the 2021 book *Law and Policy for the Quantum Age*, told the audience. "The second thing they are reasonably good at, but we don't know for how much longer, is they're reasonably good at getting funding."

Even when quantum computing becomes advanced enough to provide useful applications, the applications are likely for simulating physics and chemistry, and performing computer optimizations that don't work well with classical computing. Garfinkel said that the dearth of useful applications in the foreseeable future might bring on a "quantum winter," similar to the multiple rounds of artificial intelligence winters before AI finally took off.

The problem with the paper published earlier this month was its reliance on Schnorr's algorithm (not to be confused with Shor's algorithm), which was developed in 1994. Schnorr's algorithm is a classical computation based on lattices, which are mathematical structures that have many applications in constructive cryptography and cryptanalysis. The authors who devised Schnorr's algorithm said it could enhance the use of the heuristic quantum optimization method called QAOA.

Within short order, a host of researchers pointed out fatal flaws in Schnorr's algorithm that have all but debunked it. Specifically, critics said there was no evidence supporting the authors' claims of Schnorr's algorithm achieving polynomial time, as opposed to the exponential time achieved with classical algorithms.

The research paper from three weeks ago seemed to take Shor's algorithm at face value. Even when it's supposedly enhanced using QAOA—something there's currently no support for—it's questionable whether it provides any performance boost.

"All told, this is one of the most actively misleading quantum computing papers I've seen in 25 years, and I've seen … many," Scott Aaronson, a computer scientist at the University of Texas at Austin and director of its Quantum Information Center, wrote. "Having said that, this actually isn't the first time I've encountered the strange idea that the exponential quantum speedup for factoring integers, which we know about from Shor's algorithm, should somehow 'rub off' onto quantum optimization heuristics that embody none of the actual insights of Shor's algorithm, as if by sympathetic magic."

In geological time, yes; in our lifetime, no

On Tuesday, Japanese technology company Fujitsu published a press release that provided further reassurance that the cryptocalypse isn't nigh. Fujitsu researchers, the press release claimed, found that cracking an RSA key would require a fault-tolerant quantum computer with a scale of roughly 10,000 qubits and 2.23 trillion quantum gates, and even then, the computation would require about 104 days.

Attempts to obtain the research weren't immediately successful, and Fujitsu researchers weren't available by this story's publication. That makes it impossible for fellow researchers to know precisely what the findings are or how significant they are.

“For example, when [the Fujitsu researchers] say 10,000 qubits in the press release, do they mean logical or physical qubits?” Samuel Jaques, a doctoral student at the University of Cambridge, wrote in an email. “In my view, the best estimate for quantum factoring is still [Craig] Gidney and [Martin] Ekerå from 2020, who estimate that factoring RSA-2048 would need 20 million physical qubits and 8 hours. If Fujitsu's result drops the physical qubit count from 20 million to 10,000, that's a huge breakthrough; if instead they need 10,000 logical qubits, then that's much more than Gidney and Ekerå so I would need to check carefully to see why.”

Update: *In an email sent after this post went live, one of the Fujitsu researchers, Tetsuya Izu, senior director of data & security research, wrote:*

During the trials, we used a Shor’s algorithm and created a program to generate quantum circuits. As a next step, we used this program to generate quantum circuits for composite numbers of 9 bits and smaller, and checked actual operations (integer factorization). We then evaluated the necessary computational resources of the above mentioned quantum circuits and made estimations for the case of integer factorization of 2,048 bits composite numbers. For this reason, our estimation also uses logical qubits. We are still finalizing the research paper and unfortunately cannot provide it today. We will share the paper with you as soon as it is available.

That leads us back to the Enigma Conference and Garfinkel, who, like Jaques, said the Gidney and Ekerå findings are the best-known estimate for the breaking of RSA. Asked to respond to the oft-repeated statement that humanity is at the precipice of a large quantum computer, Garfinkel responded:

“If by large-scale you mean something that’s big enough to crack an RSA key, what do you mean humanity is on the precipice? In geological time we certainly are. In terms of the duration of the republic, sure. But in our lifetimes?”

Even when the day comes that there’s a quantum computer with the power envisioned by Gidney and Ekerå, the notion that RSA will fall in one stroke is misleading. That’s because it would take this 20 million-qubit quantum system eight hours in constant superposition to crack a single encryption key. That would certainly be catastrophic since someone might be able to use the capability to cryptographically sign malicious updates with a Microsoft or Apple key and distribute them to millions of people.

But even then, the scenario that nation-states are storing all encrypted communications in a database and will decrypt them all in bulk once a quantum computer becomes available is unrealistic, given the number of keys and the resources required to crack them all.

Over the past five years, the National Institute of Standards and Technology has run a search for new cryptographic algorithms that aren’t vulnerable to Shor’s algorithm. The process is far from finished. Last year, a candidate that had made it to the fourth round was taken out of the running after it fell to an attack that used only classical computing.

Once a post-quantum replacement is named, Garfinkel warned, “There’s going to be this mad rush to sell new things to the government so the government can immediately adopt these new algorithms. There’s just so much money to be made selling things to the government.”

Despite his insistence that the world is still decades away from being able to crack an RSA key, Garfinkel left himself wiggle room. At the same time, he said too many people focus on the risk posed by Shor’s algorithm without considering the possibility that RSA could just as easily fall from other factorization attacks posed by classical computers.

“If I was at CISA [Cybersecurity and Infrastructure Security Agency], I wouldn’t feel the need to say, ‘Don’t worry, it’s decades away’ only to risk the entire security of the United States,” he said. “But maybe we shouldn’t be moving to *just* post-quantum algorithms. Maybe we should be using the post-quantum algorithms *and* RSA in parallel because there might be a problem with the post-quantum algorithms.

3.Washington State Seeking To Be The Next Quantum Technology Cluster

https://quantumcomputingreport.com/washington-state-seeking-to-be-the-next-quantum-technology-cluster/

Several different locations in the United States are vying to be the next “Silicon Valley” where there is a concentration of companies and academic institutions that have a critical mass of expertise in a particular technology. Some of the locations that would like to achieve this in quantum tech include the Virginia/Maryland/DC area, Chicago, Colorado, New York state and others. And now the Washington Technology Industry Association (WTIA) is making a play to include the Pacific Northwest in the list.

The WTIA commissioned a study to look at the competitive situation along with the areas strengths and weaknesses for attracting more quantum activity in the region. The study points several of the area’s strengths including a substantial software and manufacturing technology presence in the Pacific Northwest including companies specializing in quantum optics and devices, a substantial base of local investors, and a good talent pool coming from the University of Washington and other schools. In addition, two big players in quantum, Microsoft and Amazon, have corporate headquarters in the Seattle area, although some of Microsoft’s research is performed in Santa Barbara near the University of California Santa Barbara and the center of Amazon’s quantum research is performed in Pasadena near Caltech. The latest company to announce they are establishing facilities in the area is IonQ which announced last week they will be opening a 65,000 square foot manufacturing facility in Bothell, Washington, a suburb of Seattle. Several organizations in the area have formed a Northwest Quantum Nexus group and recently held a Northwest Quantum Nexus Summit and Hackathon.

The report that WTIA issued made an interesting observation that Washington state is producing more quantum professionals at local universities than can be employed locally. To grow the industry are suggesting a need to focus on sectors where Washington state has strengths including health tech, agriculture tech, and cybersecurity. They would like to increase the level of cooperation with other clusters and consortiums, as well as implement programs to attract investment and retain talent.

4.What The Quantum Computing Cybersecurity Preparedness Act Means For National Security

by Skip Sanzeri
https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/?sh=5240856c368a

On December 21, 2022, President Biden signed into law H.R.7535, the Quantum Computing Cybersecurity Preparedness Act, which encourages "federal government agencies to adopt technology that will protect against quantum computing attacks."

This marks a major milestone in the global effort to develop and deploy quantum-resilient cybersecurity. It's important that the U.S. moves quickly against the coming quantum computing threat since it takes significant effort and years to upgrade existing federal and commercial technology and cryptography. Meanwhile, quantum computers are rapidly developing, with some adversarial nation-states putting tens of billions of dollars toward programs to create these very powerful machines which will break the encryption we use today.

The Act.

H.R.7535 requires federal agencies to "migrate systems to post-quantum cryptography, which is resilient against attacks from quantum computers and standard computers." To illustrate the bullish progress our federal representatives have made, H.R.7535 follows three major initiatives from earlier last year outlining how we should create a quantum-resilient U.S.

1. On January 19, 2022, the State Department issued a key initiative called the "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," stating that "Within 180 days of the date of this memorandum, agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms."

2. On May 4, 2022, the State Department published a follow-on memo called the National Security Memorandum 10 (NSM-10), "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems."

3. On November 18, 2022, M-23-02 was issued from Shalanda D. Young, the Director of the Office of Management and Budget. This memorandum describes steps for federal agencies to take as they transition to Post-Quantum Cybersecurity (PQC) by building a prioritized inventory of their cryptographic systems.

H.R.7535 now codifies that within six months, federal agencies must develop a strategy for migrating to post-quantum cryptography. In addition, it compels federal agencies to address the risk posed by weakened encryption due to the capability of a quantum computer to breach that encryption. Within 180 days of the memo (by May of 2023), the law outlines a requirement for "each agency to establish and maintain a current inventory of information technology in use by the agency that is vulnerable to decryption by quantum computers."

Most importantly, this new law has funding attached as it requires each agency to submit an estimate of the amount of money it will take for the move to quantum-safe systems.

What are quantum computers?

Quantum computers are very powerful machines that operate differently than the standard computers we use today. Standard computers struggle with certain sets of problems, one of which happens to be the base of the current cryptography that currently protects our data. The data that makes up this article and the internet it traveled across uses encryption protected by a mathematical equation using large numbers and the factors that go into those numbers. Also called prime factorization, this math problem is unbelievably difficult for classical computers to solve.

Quantum computers operate differently. Using a subatomic property called superposition, quantum computers can process problems like prime factorization and multivariate problems due to how they process data and the way they can be programmed. Unlike our classical computers, where the base elements must be zero or one, superposition allows quantum computers to take advantage of a base element being zero, one and anything in between, all at the same time.

Why do we need to act now?

It is widely understood that adversarial nation-states are building quantum computers to use as weapons. To put it as clearly as possible, the first nefarious nation-state that brings a quantum computer online with enough power to crack encryption could have unprecedented global control at its fingertips. All the private and secret information traveling over the internet will be available to anyone who has this power. This includes national secrets, healthcare data, financial and banking information, as well as access to infrastructure like energy grids, satellite communications and water supplies.

Worse yet, it is heavily documented that some nations are stealing vast amounts of data that is currently encrypted but will be decrypted when a quantum computer with enough power is available. Sometimes called “Steal Now, Decrypt Later” (SNDL), this describes stealing and storing data for a future date when there are systems that can decrypt, view and operationalize that data.

Most of these data sets need to remain secret for 25 to 75 years and would be valuable if cracked sooner. But if stolen now and decrypted within a few years by a quantum computer, an adversary would then have the capability to operationalize that data to disrupt society, steal intellectual property, gain financially or increase the chances of winning a war.

What can be done?

Most government agencies and commercial enterprises will need to take three main steps to prepare their digital infrastructure for quantum-resilient cybersecurity.

1. Start by evaluating and documenting current cryptography, which is vulnerable to quantum attacks.

2. Develop a plan to add quantum-safe cryptography where appropriate in your network, including servers, edge devices and IoT.

3. Test a quantum-safe, cryptographically agile solution in your IT infrastructure.

Selecting suitable cryptographic algorithms can be done quickly with help from a qualified consultant or vendor. However, deploying a quantum-safe security solution will take longer, depending on the size and complexity of your enterprise network.

According to Congressman Ro Khanna, who sponsored H.R.7535, “As quantum computing continues to progress, we must take steps now to protect America’s national security and economy…we have to plan ahead for potential vulnerabilities it may create.”

It is imperative that we continue this rapid progress toward a quantum-resilient technology in the U.S. as outlined by H.R.7535 so that when (not if) a bad actor has access to sufficient quantum computing power, our data, communications, systems and future will be protected.

5.Quantum Safe Cryptography – A Quantum Leap Needed Now

by Francis Sideco
https://www.forbes.com/sites/tiriasresearch/2023/01/25/quantum-safe-cryptography--a-quantum-leap-needed-now/?sh=6398e5e749ea

Whether we realize it or not, cryptography is the fundamental building block on which our digital lives are based. Without sufficient cryptography and the inherent trust that it engenders, every aspect of the digital human condition we know and rely on today would never have come to fruition much less continue to evolve at its current staggering pace. The internet, digital signatures, critical infrastructure, financial systems and even the remote work that helped the world limp along during the recent global pandemic all rely on one critical assumption – that the current encryption employed today is unbreakable by even the most powerful computers in existence. But what if that assumption was not only challenged but realistically compromised?

This is exactly what happened when Peter Shor proposed his algorithm in 1995, dubbed Shor’s Algorithm. The key to unlocking the encryption on which today’s digital security relies is in finding the prime factors of large integers. While factoring is relatively simple with small integers that have only a few digits, factoring integers that have thousands of digits or more is another matter altogether. Shor proposed a polynomial-time quantum algorithm to solve this factoring problem. I’ll leave it to the more qualified mathematicians to explain the theory behind this algorithm but suffice it to say that when coupled with a quantum computer, Shor’s Algorithm drastically reduces the time it would take to factor these larger integers by multiple orders of magnitude.

Prior to Shor’s Algorithm, for example, the most powerful computer today would take millions of years to find the prime factors of a 2048-bit composite integer. Without Shor’s algorithm, even quantum computers would take such an inordinate amount of time to accomplish the task as to render it unusable by bad actors. With Shor’s Algorithm, this same factoring can potentially be accomplished in a matter of hours.

That being said, even with this breakthrough algorithm, it still requires a quantum computer to compromise today’s encryption. This begs the question, why do we as an industry need to address this issue now, before we have practical quantum computers? First and foremost, this eventuality is not a potential but an inevitable consequence of the current progress of quantum computing. According to Dr. Michele Mosca of the Institute of Quantum Computing at the University of Waterloo, “There is a 1 in 7 chance that fundamental public-key crypto will be broken by quantum by 2026 and a 1 in 2 chance of the same by 2031.” These timeframes and the ability to store current sensitive data gives rise to the second reason – a concept called “Harvest Now, Decrypt Later.” A materially significant percentage of sensitive data will still be relevant in this time frame – and that is data that is not currently protected against quantum-based decryption techniques. This concept allows bad actors to “harvest” the data now and act upon it later when technology has matured to make the decryption of that data practical and viable.

As such, the National Institute of Standards and Technology (NIST) has been leading the charge since 2016 for the standardization of quantum safe cryptography. After multiple rounds of algorithm submissions, four finalists were selected in July of 2022 with three of those four algorithms being created by IBM along with their industry and academic partners. This is not entirely surprising given that aside from their work on quantum safe encryption, IBM is also a driving force in quantum computing and plans to introduce a new 4k qubit system by 2025 and is even working on solving the technical issues to eventually get to a 1 million qubit system. Between these four algorithms, public-key encryption and key establishment as well as digital signatures are addressed.

These quantum-safe cryptographic algorithms could not have come at a better time. Digital infrastructure such as passports, vehicles, critical infrastructure and public transportation take a long time to upgrade, with some time periods spanning 10-50 years. Use of that digital infrastructure is already pervasive and will only continue to exponentially increase as new use cases and applications are introduced. The more we rely upon digital infrastructure and the more sensitive data we store in that digital infrastructure, the larger the motivation for bad actors to compromise the encryption that protects that data. The industry is poised to take a quantum leap in both cryptography and computing. The time is now to take that leap.

6.Quantum Computing Is Coming, And It’s Reinventing The Tech Industry

https://www.forbes.com/sites/qai/2023/01/24/quantum-computing-is-coming-and-its-reinventing-the-tech-industry/?sh=5ebd543214de

Quantum computing is an idea that has long been in the realm of science fiction. However, recent developments have made it seem more and more like a reality.

The rise of easily accessible quantum computing has significant implications for the tech industry and the world as a whole. With potential impacts in things like cybersecurity, simulations and more, investors are watching this industry closely (and getting invested).

What is quantum computing?

Quantum computing relies on quantum mechanics, a fundamental theory of physics that describes how the world works at the level of the atom and subatomic particles, to solve problems that traditional computers find too complex.

Most quantum computers rely on the “quantum bit” or qubit. Unlike traditional bits in a computer, which are set to 0 or 1, qubits can be set to zero, one or a superposition of 0 and 1. Though the mechanics behind this is highly complex, qubits allow quantum computers to process information in a fraction of the time a traditional computer could.

To offer an idea of the scale, 500 qubits can represent the same information as 2^500 normal bits. While a typical computer would need millions of years to find all the prime factors of a 2,048-bit number (a number with 617 digits), a quantum computer can do the job in minutes.

Modern quantum theory was developed in the 1920s. Computers appeared shortly after that, and both technologies played a role in World War II. Over time, physicists began to merge the two fields of quantum theory and computing to create the field of quantum computing.

1998 saw the development of a two-bit quantum computer, which serves as a proof of concept for the technology. Further developments have increased the bit count and reduced the rate of errors.

Researchers believe that problems currently too large to be solved by traditional computers can be solved using quantum computers.

Recent developments

Given the substantial improvements that quantum computing can provide to computing power, research into quantum computers has been going on for decades. However, important breakthroughs have been seen in recent years.

Last week, Australian engineers announced the discovery of a way to control electrons within quantum dots that run logic gates without the need for a large, bulky system. This could help with building quantum computers that are reasonably sized.

Also, researchers at MIT recently developed an architecture for quantum computers that will allow for high-fidelity communication between quantum processors, allowing for the interconnection of multiple processors.

This allows for “modular implementations of larger-scale machines built from smaller individual components,” according to Bharath Kanna, a co-lead author of the research paper describing this breakthrough.

“The ability to communicate between smaller subsystems will enable a modular architecture for quantum processors, and this may be a simpler way of scaling to larger system sizes compared to the brute-force approach of using a single large and complicated chip.”

Furthermore, a Maryland-based company IonQ recently announced a 65,000-square-foot facility that it will use for manufacturing and production. The factory will be located in Bothell, WA and is the first dedicated quantum computer manufacturing facility in the United States.

How will it impact the tech industry?

Quantum computing could have massive impacts on the tech industry and the world.

One of the biggest impacts will be in the world of cybersecurity. The Department of Homeland Security believes that a quantum computer could be able to break current encryption methods as soon as 2030.

Without major developments in cryptography or a slowdown in quantum computing technology advances, we could be less than a decade away from malicious actors being able to view everything from people’s personal information to government and military secrets.

Some groups are already participating in “Store Now, Decrypt Later” attacks, which steal encrypted data and store it with the expectation that they’ll be able to crack the encryption at a later date.

Quantum computing could also have major effects on the medical industry. For example, quantum machines could be used to model molecular processes. This could assist with breakthroughs in disease research and speed up the development of life-saving drugs.

These simulations could have similar impacts in industries that rely on materials science, such as battery making. Even the financial sector could benefit from the technology, using simulations to perform risk analysis more accurately and optimize investment portfolios.

Given its world-changing capabilities, it's no surprise that governments have made major investments in the technology, with more than $30 billion going into research programs across the globe.

What it means for investors

Quantum computing has the potential to impact almost every industry across the globe. Beyond impacting the tech industry, it could create shockwaves in the medical and financial industry while leading to the development of new products or materials that become a part of everyday life.

Given the relative youth of the technology, it can be challenging for investors to find ways to invest directly in quantum computing. Instead, they may look for investments in businesses that have an interest in quantum computers and that are poised to benefit from their development, such as pharmaceutical companies.

The bottom line

The rise of quantum computing could mean that the world will look very different just a few years from now. Investors will be looking for ways to profit from this game-changing technology, and the opportunities will be plentiful.

7.French Startup Raises $5M To Make Quantum Internet Dream Come True

by Editorial Team
https://techfundingnews.com/french-startup-raises-5m-to-make-quantum-internet-dream-come-true/

Welinq, a Paris-based startup that operates on quantum memory technology to scale up quantum computing and enable quantum internet deployment, has raised €5M funding.

Quantonation, the first venture capital fund dedicated to quantum technologies, led the pre-seed round, with participation from Luxembourg-based Runa Capital and support from the Paris Region, the French National Quantum Initiative, the French Banque Publique d'Investissement (BPI), and the European Commission.

With the money raised, the team intends to commercially launch its first product, a highly effective quantum memory, in infrastructures for quantum computing and quantum communication. Basically, the French quantum tech wants to deploy the world's most efficient quantum memories at industrial standards in quantum computing and quantum communication infrastructures.

Welinq's quantum memories allow for the on-demand storage and release of quantum information without changing its fundamental characteristics. The team has demonstrated with 90% the world record in storage-and-retrieval efficiency (a parameter indicating how much of the information is retained through the process without being lost on the way) with a qubit fidelity above 99% by using laser-cooled neutral-atom technology. The group is currently working on its first product, a highly effective quantum memory that will be deployable, transportable, and integrated into infrastructures for quantum computing and quantum communication.

The Laboratoire d’Informatique de Sorbonne Université (LIP6), a synergistic, multidisciplinary research centre and France’s largest laboratory in computer science, and the Laboratoire Kastler Brossel (LKB), a leading actor in fundamental physics of quantum systems, are the two prestigious French laboratories that gave rise to the Welinq technologies. Together, they have won three Nobel prizes and five CNRS Gold Medals.

“Quantum memories have been identified today as the key missing hardware for the scale-up of quantum technologies. Not only must these devices be deployed on the market at the earliest, but they also need to show extremely high performance and robustness if we want them to truly impact industry and society. We are happy to be joined in this project by investors with strong expertise in quantum technologies and who are sharing our ambitions for the future of quantum technologies,” says Tom Darras, CEO and co-founder of Welinq.

“At Quantonation, we believe that the development of efficient quantum interconnects is a pillar for the whole quantum infrastructure and a path to accelerate real-world applications. The founding team has groundbreaking expertise and a clear path to be impactful. We are excited to start this journey with Welinq,” says Christophe Jurczak, partner at Quantonation

Dmitry Galperin, a Berlin-based General Partner at Runa Capital adds, “When I first met Welinq’s team I was very impressed by their unique technology and the major impact that it can have on quantum computing scale-up. We are happy to stand with this founding team that gathers diverse backgrounds and a common strong ambition for the future of quantum interconnects.”

Welinq, a company established in 2022, makes it easier to connect quantum computers remotely while maintaining their distinctive characteristics. This might make it possible for researchers to build much bigger quantum systems without any problems.

To address the scaling-up of quantum computing, Tom, Julien Laurat, Eleni Diamanti, and Jean Lautier-Gaud—who had previously collaborated in their academic careers—decided to join forces and found Welinq. Their understanding of interconnects as the central component of long-distance quantum information networks and a privileged way to scale up quantum computing beyond the thousands of qubits range quickly became crystal clear.

The Welinq CEO Tom Darras received his PhD in quantum physics from Sorbonne Université after earning an engineering degree in Physics at ESPCI Paris. He worked on quantum teleportation protocols for quantum interconnects. Following his PhD, he moved from academia to entrepreneurship, co-founding Welinq in 2022. As a young physicist and entrepreneur, he thrives on taking on ambitious technological challenges in order to turn proof-of-concept laboratory experiments into real-world solutions that will have a significant impact on science and industry. He was named Grand-Prix of the French Innovation i-Lab competition in 2022.

The team currently consists of 8 members (2 women and 6 men) of four different nationalities (French, Italian, Greek and Indian).

8.Pentagon Must Act Now On Quantum Computing Or Be Eclipsed By Rivals

by Freddie Hudson
https://www.c4isrnet.com/thought-leadership/2023/01/20/pentagon-must-act-now-on-quantum-computing-or-be-eclipsed-by-rivals/

As quantum computers continue to advance and become more powerful, they present a significant threat to the Department of Defense's cybersecurity assurance.

When former Pentagon's Chief Data Officer, David Spirk, left his post in March 2022, he did so with a warning: "I don't think that there are enough senior leaders getting their heads around the [cybersecurity] implications of quantum… I think that's a new wave of computers that, when it arrives, is going to be a pretty shocking moment to industry and government alike."

Quantum computers have the ability to process information much faster than classical computers, making them capable of cracking the secure encryption algorithms relied on to protect information today. This could allow adversaries to access sensitive military intelligence, disrupt communication networks, and even disable military systems.

In late 2021, the head of the NSA's Cybersecurity Directorate signaled that developing next-generation cryptologic systems to secure weapon systems from foreign adversaries was a top priority. In a fact sheet published that year, the NSA stated that "the impact of adversarial use of a quantum computer could be devastating to National Security Systems."

The battle for quantum supremacy is already under way, and is set to fundamentally change the defense sector as the technology edges towards maturation.

The quantum threat is closer than you think

Many experts, including Spirk, believe that military applications for quantum computing could be less than 10 years away.

Case in point: according to the Pentagon's annual report on Chinese military power, China recently designed and fabricated a quantum computer capable of outperforming a classical high-performance computer for a specific problem.

This is also why DARPA announced the 'Underexplored Systems for Utility-Scale Quantum Computing' (US2QC) program to explore potentially overlooked methods by which quantum computers could achieve practical levels of utilization much faster than current predictions suggest.

The White House recently signed the Quantum Computing Cybersecurity Preparedness Act into law, signaling that it regards quantum as a serious issue. The act addresses the migration of executive agencies' IT systems to post-quantum cryptography (PQC) - encryption which is secure from attacks by quantum computers because of the advanced mathematics underpinning it.

As major powers like China, under its Digital Silk Road initiative, continue to accelerate investment into advanced technologies like AI and quantum computing, the US risks being left behind if it does not pay equal attention to the quantum opportunity - and to the quantum threat.

The need for action is all the more urgent because of the looming threat of 'harvest now, decrypt later' attacks, by which adversaries can gather sensitive data today to decrypt as soon as they have their hands on a sufficiently powerful quantum computer.

Time is running out for the DoD

The defense sector needs to take the threat of quantum computers seriously because they have the potential to greatly impact national security.

Encryption is a crucial tool for protecting sensitive military information, and if quantum computers are able to break current encryption algorithms, this could compromise the security of classified documents, strategic plans, and even communication networks. This could potentially give adversaries an advantage in military conflicts and put US military personnel at risk.

In addition to the potential impact on national security, the defense sector also has a responsibility to protect the personal information of military personnel and civilians. Quantum computers could potentially be used to steal sensitive personal information, such as social security numbers, as well as medical and financial information.

As DoD moves from network-centric operations to data-centric operations, PQC implementation becomes even more relevant, regardless of whether the data comes from the cloud or any other source. DoD's Joint All Domain Command and Control (JADC2) and Joint Cloud Computing concepts, network modernization etc. will all require post-quantum cryptography for cybersecurity assurance.

Quantum computers also have the ability to perform complex calculations at a much faster rate than classical computers, which could allow them to disable or manipulate military systems. This could potentially disrupt communication networks, navigation systems, and even weapons systems, leading to potential loss of lives and damage to military assets.

First-mover advantage

In July last year, the National Institute of Standards and Technology announced a major milestone in its efforts to standardize post-quantum cryptography algorithms.

New draft standards are a welcome arrival and will hopefully dispel any hesitation about putting concrete transition roadmaps in place. But the bigger picture is that encryption standards are going through their biggest change in decades, and post-quantum cryptography will soon be essential for all businesses hoping to work with the US government. Up to $3 billion of federal quantum projects are now either in operation or planned, including a $1.2 billion National Quantum Initiative.

The advent of quantum technology converges with the race for global tech supremacy as well as a period of turbulent geopolitics. The longer the government and businesses wait to act, the greater the potential harm.

9.Tackling Quantum Computing Attacks With Post-Quantum Cryptography And Confidential Computing

by Avishai Sharlin
https://venturebeat.com/security/ibm-quantum-computing/

The Fast Mode spoke to Avishai Sharlin, Division President at Amdocs Technology on new encryption technologies and their impact on today's networks. Avishai joins us in a series of discussions with leading vendors in the traffic management, service assurance, traffic monitoring, analytics, policy control and network security space, assessing various attributes of encryption, its benefits as well as the challenges it poses, specifically loss of visibility that makes networking increasingly complex.

Tara: How important is encryption for today's applications?

Avishai: In an era when data is the world's most valuable and vulnerable currency, encryption has never been more important – particularly given the ever-evolving nature of the threats to application security. For example, it is feared that recent advancements in quantum computing can seriously risk the encryption standards we have today, and that in the next one to two years quantum computing will be powerful enough to break almost all existing security cryptography algorithms. Indeed, it has already been widely reported that hackers are purposefully stealing highly encrypted data that they cannot decrypt today and storing it as they will be able to decrypt it in the next year and beyond using new quantum computing techniques. When you take a step back, that's an alarming prospect for the industry and society at large. In fact, the risk of quantum computing is already here: a Chinese research group recently released a paper claiming that if it had access to a Western quantum computer today (such as IBM Osprey), they have devised a method whereby they can brute-force attack and decrypt the widely-used RSA 2048bit encryption.

Application use creates output, which we store and call data. Applications also ingest existing data such as sensitive customer information (PII data) for processing and enabling services. Encryption is a key operational task we must execute to ensure that our application data will not be read by a third party via theft, leak, or a breach. The move to the public cloud, a shared infrastructure, further emphasizes the importance of guarding and protecting data. In public cloud environments, servers are shared between multiple customers and data is stored on storage systems that are also shared between many customers. Although dedicated infrastructure is possible in the public cloud it's extremely expensive.

Hence, to protect data on the public cloud and even on-premise, encryption is a mandatory operation and process that must be executed for all data in transit (over the wire, via HTTPS application wise), and at rest (when the data is stored to disk). This also relates to low-code applications: there is no exception here. The way we develop an app (low code) must not impact our ability to ensure the data the app generates is secure and encrypted. It's important to remember that on public clouds there is a shared responsibility model – the public cloud provider provides the infrastructure and required services to run an app, but the application security and its data is not within its hands.

Tara: The evolution of encryption technologies – where are we headed?

Avishai: To fight off quantum computing brute-force attacks, new algorithms for encryption are required. Post-Quantum Cryptography (PQC), where new chosen algorithms by NIST, will replace existing encryption algorithms so data remains protected in the quantum computing era. This will have a serious impact industry-wide, as code change is required for this to happen at the application level (if the application uses crypto libraries and encrypts data on its own). For example, Java-based apps will require an updated OpenJDK and new Crypto library/APIs to support these new algorithms, and the application must update its code base to use these new Crypto APIs.

To enable encryption and secrets (passwords), encryption keys must be guarded and never stored in the open on servers or disks next to the application or where it is stored for execution. As public cloud adoption progresses, services and applications are protecting their keys in managed services such as key management systems in the public cloud. The application interacts with the system to fetch the encryption keys over the wire on a secure link for encryption operation. Key management systems can also be used to execute the encryption process, allowing the application developer to offload it.

Last, public clouds allow applications to utilize hardware security modules (HSMs) via APIs. These super-hardened encryption servers are similar to key management systems but also have the required computing power to encrypt data on behalf of the application. Applications interact with the module for all cryptographic operations, and the encryption keys never leave the HSM. A dedicated HSM provides the most secure way to encrypt and protect data in the cloud.

Confidential computing is an evolution of offerings we have in public clouds and on premise. New advanced processors and chipsets provide built-in memory encryption capabilities of the server memory where we host our applications. New processors from AMD and Intel allow encryption of the entire memory of a server or specific VMs used in shared infrastructure such as the public cloud or virtualization platforms, in real time without any performance degradation. This ensures that the application memory running in that VM is fully encrypted.

Confidential computing also provides new ways for applications to store sensitive data inside the secure enclave in modern CPUs. This is a highly secure and restricted area in the CPU, to which only the CPU can have access. An encryption key can be stored in the processor secure enclave and only the processor and the app can access it.

We are seeing a call from the industry for organizations to start adopting this technique to better protect their data. This means we will likely see the widespread adoption of new algorithms and ciphers to safeguard data in ways that cannot be broken by the quantum computing power we have today and in the future.

10.Quantum Computing: Examining The Quantum Computing Cybersecurity Preparedness Act

by Jacob W. S. Schneider
https://www.hklaw.com/en/insights/publications/2023/01/quantum-computing-examining-the-quantum-computing-cybersecurity

In the waning days of 2022 and the 117th Congress, President Biden signed H.R.7535, the Quantum Computing Cybersecurity Preparedness Act, into law. The law recognizes the future threat that quantum decryption poses to federal administrative agencies and orders an examination of the agencies' data cryptography to prepare for a time, perhaps many years from today, when quantum computing is capable of decrypting that data. This post examines the new law as well as what motivated Congress to act.

Why Prepare Cybersecurity for Quantum Computing?

Nearly everything sensitive that is transmitted or stored on computers is encrypted. For example, encryption protects our bank accounts, health records and app-based messaging. Encryption takes a block of readable data and makes it unreadable to everyone but those users who hold a cryptographic key and can decrypt it. As with a physical bike lock, encryption schemes can be decrypted even without the key. Also like a physical bike lock, as an encryption scheme becomes more and more complex, the likelihood that anyone could realistically decrypt it goes down.

Certain types of quantum computers are likely to be excellent encryption "lock–pickers" in the future.

The math tells us that if such computers were ever built to scale – an event that is difficult to predict but could be over a decade away – then they would be efficient at decrypting the most widely used encryption schemes that exist today. In effect, using the most popular, modern encryption schemes is like buying an expensive bike lock with the understanding that, at some unknown point in the future, it will be worthless against thieves.

Developing Post-Quantum Cryptography / Quantum-Safe Algorithms

Quantum computers are chess grandmasters who cannot tie their shoes and forget where they put their wallets: They are very good at a certain class of problems, but lousy at others. (A quantum computer would have a hard time, for example, doing something as basic as rendering this webpage.) As a result, there is math that quantum computers are no better at than classical computers, and encryption schemes that rely on that math are more resilient to a quantum decryption attack.

In 2016, the National Institute of Standards and Technology (NIST) began a lengthy public competition to develop these "post-quantum" cryptographic schemes, which are a subset of "quantum-safe algorithms." NIST described the quantum decryption problem as its motivation for the project:

> *In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere.*

NIST's stated goal was "to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.”

In 2022, the ongoing project identified several promising candidate algorithms, including CRYSTALS-Kyber (for key establishment) and CRYSTALS-Dilithium (for digital signatures). NIST is currently working to standardize these algorithms for wide-scale use.

The Quantum Computing Cybersecurity Preparedness Act

Quantum decryption could also compromise government secrets. So, with quantum decryption on the horizon, Congress passed, and the President signed into law, the Quantum Computing Cybersecurity Preparedness Act to mitigate the looming threat.

The Act acknowledges the threat that quantum computing raises for national security:

(1) Cryptography is essential for the national security of the United States and the functioning of the economy of the United States.

(2) The most widespread encryption protocols today rely on computational limits of classical computers to provide cybersecurity.

(3) Quantum computers might one day have the ability to push computational boundaries, allowing us to solve problems that have been intractable thus far, such as integer factorization, which is important for encryption.

(4) The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers, and wait until sufficiently powerful quantum systems are available to decrypt it.

Sections 2(a), 3(d)(9) (defining a "quantum computer" as "a computer that uses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations").

The Act requires that the Director of the Office and Management and Budget (OMB) develop and issue guidance for administrative agencies "on the migration of information technology to post-quantum cryptography." Section 4(a). This guidance must include "a requirement for each agency to establish and maintain a current inventory of information technology in use by the agency that is vulnerable to decryption by quantum computers." Section 4(a)(1).

Following that guidance, agencies will then report back to the OMB with their inventory of IT vulnerable to quantum decryption. Section 4(b). One year after NIST issues its post-quantum cryptography standards, OMB will issue further guidance to prepare agencies for the migration of their data to the new, quantum-resilient standards. Section 4(c). Throughout this period, and for the following five years, OMB will report back to Congress on the migration's progress. Section 4(e). This lengthy period acknowledges the difficulty that agencies, many of which still rely on older, legacy systems, will have in overhauling their encryption schemes.

The Act exempts all national security systems. Section 5. Migrating these systems to post-quantum cryptography, however, is already underway.

While the Act will go a long way toward strengthening agency data against a quantum attack, in some respects, the cat is already out of the bag. Today's hackers can obtain encrypted data and store it for years, knowing that a future quantum computer will be able to decrypt it. This technique is sometimes called "harvest now, decrypt later," and the Act cannot protect already compromised data from later decryption. Still, the government's acknowledgement and mitigation of future threats is an important step toward protecting its data in the future.

11.IBM: Quantum Computing Poses An ‘Existential Threat’ To Data Encryption

by Tim Keary
https://venturebeat.com/security/ibm-quantum-computing/

For years, encryption has played a core role in securing enterprise data. However, as quantum computers become more advanced, traditional encryption solutions and public-key cryptography (PKC) standards, which enterprise and consumer vendors rely on to secure their products, are at serious risk of decryption.

Today, IBM Institute for Business Value issued a new report titled Security in the Quantum Era, examining the reality of quantum risk and the need for enterprise adoption of quantum-safe capabilities to safeguard the integrity of critical applications and infrastructure as the risk of decryption increases.

The report argues that quantum computing poses an “existential risk” to classical computer encryption protocols, and notes that cybercriminals are potentially already exfiltrating encrypted data with the intention of decrypting it once quantum computers advance as part of “harvest now, decrypt layer attacks.”

The problem with traditional encryption and quantum computing

One of the central limitations of traditional cryptographic protocols like RSA is that they’re reliant on mathematical problems like the factorization of large numbers, which are simple enough for a quantum computer to solve with brute force.

With a quantum computer, cryptographic protocols "can in theory be solved — and solved within a few hours — with the help of Shor's algorithm," the report said. "This makes protocols like RSA an insufficient cryptographic scheme in a future where quantum computers have reached their full potential."

While this process hasn't taken place just yet, more and more organizations are taking the risk of this decryption seriously. In December 2022, President Biden signed the Quantum Computing Cybersecurity Preparedness Act encouraging government agencies to adopt technology that's resistant to post-quantum decryption.

Likewise, last year NIST concluded its search to identify quantum-resistant algorithms that had been ongoing since 2016, choosing four algorithms as finalists, and selecting CRYSTALS-Kyber, a public-key encryption algorithm and CRYSTALS-Dilithium a digital signature algorithm, as its top two chosen standards.

Investing in quantum security is now becoming a necessity for enterprises. From our point of view at IBM, it's important for CISOs and security leaders to understand quantum-safe cryptography," said Dr Vadim Lyubashevsky, cryptography research at IBM Research.

"They need to understand their risk and be able to answer the question: what should they prioritize for migration to quantum-safe cryptography? The answer is often critical systems and data that need to be kept for the long term; for example, healthcare, telco, and government-required records," Lyubashevsky said.

IBM's lattice-based approach to quantum-safe encryption

With the global quantum cryptography market expected to grow from $89 million in 2020 to $214 million by 2025, IBM has been active in establishing itself as a leader within the space alongside other providers like Intel, which has helped contribute to NIST's post-quantum cryptography standards.

Just last year, IBM launched IBM z16, a quantum-safe, AI-driven data inference-optimization solution designed for processing mission-critical data. The company had also contributed to three of the four post-quantum algorithms chosen by NIST.

Part of IBM's quantum-safe strategy is to use lattice-based cryptography, a method for constructing security primitives that's based on the geometry of numbers, which can be used to construct encryption protocols that are harder for quantum computers to crack than those that rely on factorization.

IBM notes that this approach first emerged in the 1990s out of two research papers, Brown University's NTRU: A new high speed public key cryptosystem by Jeffrey Hoffstein, Jill Pipher and Joseph Silverman; and IBM scientist Miklos Ajtai's Generating Hard Instances of Lattice Problems.

12.Getting America's Skies Quantum Ready

by Arthur Herman
https://www.forbes.com/sites/arthurherman/2023/01/17/getting-americas-skies-quantum-ready/?

sh=5a2783953302

The air traffic shutdown last week, the worst since 9/11, represents a salutary warning to government as well as private industry. If you thought our air traffic infrastructure is vulnerable to hackers, you're right. Between outdated computer systems and inadequate cybersecurity, the world of air travel offers multiple points of entry for the current hacker or a future quantum computer attack. Closing those points, and getting serious about making our skies cyber and eventually quantum-safe should be a major priority for a Secretary of Transportation—far more, frankly, than any climate change agenda.

The truth is, those malicious attacks have been going on for a while.

- On May 7, 2009, hackers got into the FAA computer system, and stole the personal of some 45,000 employees.
- In 2013 a malicious phishing scam targeted 75 US airports.
- On February 23, 2021, NASA and FAA were both hacked by Solar Wind.
- On October 10, 2022, Russian hackers knocked key U.S. airports offline, including LAX and La Guardia, O'Hare and Midway airports in Chicago.

That's what can happen if someone targets more stationary targets. Airliners themselves are particularly vulnerable, according to Neucrom Security Labs research, thanks to their WiFi services. By cracking open access to the thousands of accounts using WiFi in the air, or hacking into airline terminals on the ground, hackers will have a gold mine rich with what they are looking for, namely mountains of data, both proprietary and personal. It's not just a U.S. problem. The European Organisation for the Safety of Air Navigation, or Eurocontrol, published a report in July 2021, "Airlines under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?"

But the threat of quantum computer attack goes far beyond stolen identities, cancelled flights, or even airport shutdowns. An extended quantum threat can disrupt air travel for protracted periods, and generate aerial chaos on a global scale. It could mean downed planes, endless routing chaos, and collisions between commercial flights and mission-critical military aircraft in a time of war or national emergency.

For example, the system that went down a week ago was the Notice to Air Missions (NOTAM). It sends alerts to pilots to let them know of conditions that could affect the safety of their flights. It is separate from the air traffic control system that keeps planes a safe distance from each other, but a critical part of guaranteeing air safety.

Imagine a quantum hack that sends false notices to pilots that send them and their passengers on a deadly journey, all based on false data or weather information, and all using the same system that's designed to keep airliners in the sky, instead of crashing them to earth.

The heart of America's air travel infrastructure, the Air Traffic Control system itself (ATC), is kept offline to avoid the threat of malicious attack by state or non-state actors. But some components do communicate via the Net, for example for system maintenance, while ATC's Next-Gen modernization program will rely on IP-based networks in order to communicate, which opens another portal to malicious intrusion, especially by a future quantum computer that can punch through any existing encryption.

Fortunately, this White House has gotten serious about the quantum computer threat. So has Congress. Now the Transportation Department needs to take the lead in adopting the zero trust cybersecurity standards required by executive order, including adopting quantum-safe protocols.

What can the Transportation Secretary and his cybersecurity staff do?

- **First**, post an accelerated timeline for migration of all air travel-related communication and computer systems to post-quantum cryptography, i.e. the large quantum-resistant algorithms recently standardized by NIST, which can also protect against current hackers.
- **Second**, issue a Request For Information (RFI) to cybersecurity companies familiar with the quantum threat, on how to use those NIST standards to map out a strategy for guarding against future quantum hackers in the event of national emergency or time of war.
- **Third**, meet with those quantum cybersecurity companies who can provide the right flexibility and resilience that a full-court press post-quantum cyber regime will need, including regular upgrading of key existing systems and installing of quantum-safe encryption for future ones.
- **Fourth**, make sure other parts of the US transportation grid—rails, subways, highways—are migrating toward post-quantum solutions, as well; including where—as with industrial systems and the power grid—using quantum cryptography may be the better answer than PQC.

Our Transportation Secretary, and his counterparts in relevant committees in the Senate and the House, need to be constantly thinking about how keep our skies safe from malicious cyberattack. The advent of encryption-breaking quantum computers will make that task all but impossible, unless we take steps now to match the quantum-safe tools we already today, to the systems that will need them tomorrow.

13.Post-Quantum Cybersecurity Threats Loom Large

by Help Net Security
https://www.helpnetsecurity.com/2023/01/16/post-quantum-cybersecurity-threats/

A new Zapata Computing report reveals a deepening commitment from enterprises that points to a maturing industry with widespread, global interest and increased urgency regarding post-quantum cybersecurity threats.

The growing interest in quantum is translating into spending, demonstrated by 71% of quantum-adopting enterprises surveyed having current quantum computing budgets of more than $1 million. This finding represents a 2.5X increase over 2021, where only 28% of quantum-adopting respondents indicated that they had a quantum computing budget of more than $1 million.

Considering this net-positive shift in budgets, it's no surprise that 74% of enterprise leaders have adopted or are planning to adopt quantum computing. Interestingly, nearly 30% of respondents that have adopted or plan to adopt quantum computing expect to see a competitive advantage due to quantum computing within the next 12 months.

This represents more than a sevenfold increase year-over-year from 2021 (4%) and highlights the growing commitment to near-term quantum computing initiatives as the technology continues to mature.

"We're getting a unique glimpse into the quantum adoption mindset of global enterprise executives, which mirrors what we're seeing in our customer base," said Christopher Savoie, CEO of Zapata Computing.

“These findings become more interesting when compared to the data we saw last year. Over the past 12 months, we’ve seen significant new developments in technology, particularly generative AI, and near-term advantages from quantum-inspired technologies that are fueling the momentum for quantum computing planning and adoption. As a result, more enterprises are exploring what’s possible with the hybrid quantum classical compute capabilities of today and how the potential of quantum computing may impact their competitive position — and ultimately their business results,” Savoie continued.

Machine learning and data analytics continue to be the leading quantum use cases

Beyond one-off experiments, enterprises are focused on well-defined use cases and problems, with 71% of quantum-adopters indicating they were focused on machine learning/data analytics problems, up from 55% in 2021.

Vendor lock-in concerns are nearly universal

91% respondents indicate they are concerned about vendor lock-in, which becomes a concern when a technology is on the verge of being used to address real-world, commercial-grade challenges. It’s too early to tell which hardware architecture will prevail, and adopters are wary of implementing a paradigm that may not be the best for their needs in the long term.

Post-quantum cybersecurity threats

In addition to being the biggest challenge to quantum adoption cited by respondents, 65% of respondents are extremely or very concerned about post-quantum cryptography (PQC), and 63% of respondents are actively working with a vendor to prepare. The concerns reflect both the magnitude of the threat posed by quantum computers and the absence of clearly reliable solutions.

Integration challenges remain an obstacle to adoption

The complexity of integrating quantum computing with existing IT stacks fell just behind security concerns as the top hurdle to quantum adoption. The persistence of this challenge was also reflected by the top considerations for selecting quantum vendors, with 51% prioritizing easy-to-use solutions and 50% prioritizing easy integration with existing IT.

Expectations of better business results drive quantum adoption

The top motivation for exploring quantum computing is driving better performance and business results, with 70% of quantum-adopting respondents citing this motivation, up from 60% in 2021.

Enterprises get tactical about quantum adoption

Enterprises are taking tactical steps to make quantum computing a reality, with respondents noting that they are building new applications (48%), running experiments on quantum hardware or simulators (62%), and experimenting and building proofs of concept (51%).

Each of these steps saw increased activity by enterprises in 2022 compared with the previous year. The biggest shift was towards running experiments on quantum hardware, which grew from 48% of enterprises in 2021 to 62% in this year’s study.

Quantum adoption outpaces AI adoption

Enterprise leaders say they are adopting quantum technology more quickly than they did artificial intelligence. 49% of respondents say they are deploying quantum more quickly than they did with AI, with only 17% indicating they're taking a slower pace.

14.Computers Need To Make A Quantum Leap Before They Can Crack Encrypted Messages

by John Naughton
https://www.theguardian.com/commentisfree/2023/jan/14/computers-need-to-make-a-quantum-leap-before-they-can-crack-encrypted-messages

Security in a digital world requires that our communications are safe from digital eavesdroppers. The way we do that is to encrypt our messages using mathematical tools. The most powerful of these use trapdoor functions – that is, ones that work easily in one direction (making encryption easy) but not in the other (making decryption difficult).

Trapdoor functions utilise a property of multiplication – its asymmetry. It's simple to multiply two numbers together, for example, 971 and 1,249, to get 1,212,779, but it's quite hard to start with 1,212,779 and work out which two prime numbers (its factors) have to be multiplied to produce it. And the task becomes exponentially harder the bigger the original numbers are. Which is why, up to now, computer scientists believe that it's impossible *in practice* for a conventional computer, no matter how powerful, to factorise any number that's longer than 2,048 bits. Why so? Because it would take it 300tn years, or about 22,000 times longer than the age of the universe (to use just one of the popular analogies), for the machine to crack the problem.

This explains why the 2,048-bit limit is the basis for the most commonly used form of asymmetric encryption today, the RSA system, which relies on the difficulty of factoring the product of two large prime numbers, namely, numbers that are divisible only by themselves and 1. That doesn't mean that RSA encryption is unbreakable (mathematicians never say never) – just that it won't be broken in the near future and so the world can rest assured that it'll be good for, say, the next 25 years.

Being an alert reader, you will already have spotted the critical fly in this soothing ointment – the assumption that the computers we will be using in 25 years' time will be similar to the ones we use today. Since the early 1980s, physicists and computer scientists such as Richard Feynman, Paul Benioff, Yuri Manin (who died last weekend at the age of 85) and Britain's David Deutsch have been thinking about a different idea – using some ideas from subatomic physics to design a new and very distinct kind of computing engine – a quantum computer. In 1985, Deutsch published a proposal for one. And in recent times, companies such as Google and IBM have begun building them.

Why is that relevant? Basically because quantum computers are potentially much more powerful than conventional ones, which are based on digital bits – entities that have only two possible states, on and off (or 1 and zero). Quantum machines are built around qubits, or quantum bits, which can *simultaneously* be in two different states.

At this point, you may be anxiously checking for the nearest exit. Before doing so, remember that to understand subatomic physics you need first of all to divest yourself of everything you think you know about the physical world we ordinary mortals inhabit. We may sometimes be rude about people who believe in fairies, but particle physicists fervently believe in the neutrino, a subatomic particle that can pass right through the Earth without stopping and we take these scientists seriously.

Way back in 1994, the mathematician Peter Shor showed why we might be right to do so. Any entity equipped with a powerful enough quantum computer, he argued, could potentially break most commonly used cryptographic codes, including RSA. The problem was that the dream machine would need a billion qubits to do the job reliably. Other researchers recently calculated that it would need "just" 20m qubits but could do the requisite calculation in about eight hours.

However, a new paper by a group of Chinese researchers claiming that they can break 2,048-bit RSA has caused a brief flurry in cryptographic circles. It was rapidly debunked by a couple of experts, including US computer scientist Scott Aaronson, who described it as "one of the most actively misleading quantum computing papers I've seen in 25 years and I've seen… many".

There will be more where that came from. So it's time for a reality check. Quantum computers are interesting, but experience so far suggests they are exceedingly tricky to build and even harder to scale up. There are now about 50 working machines, most of them minuscule in terms of qubits. The biggest is one of IBM's, which has – wait for it – 433 qubits, which means scaling up to 20m qubits might, er, take a while. This will lead realists to conclude that RSA encryption is safe for the time being and critics to say that it's like nuclear fusion and artificial general intelligence – always 50 years in the future. That doubtless will not prevent Rishi Sunak from declaring his intention to make the UK "a world leader in quantum" but my money is on RSA being secure for my lifetime – and possibly even Sunak's.

15.Vulnerabilities In Cryptographic Libraries Found Through Modern Fuzzing

by Zeljka Zorz
https://www.helpnetsecurity.com/2023/01/13/fuzzing-cryptographic-libraries/

Recently patched vulnerabilities in MatrixSSL and wolfSSL, two open-source TLS/SSL implementations / libraries for embedded environments, have emphasized the great potential of using fuzzing to uncover security holes in implementations of cryptographic protocols.

CVE-2022-43974 and CVE-2022-42905

CVE-2022-43974 is a buffer overflow vulnerability found in MatrixSSL versions 4.5.1-4.0.0 that could allow information disclosure and remote code execution.

It was discovered and reported by Robert Hörr and Alissar Ibrahim, security evaluators with Deutsche Telekom's IT Security Evaluation Facility, and has been patched in version 4.6.0, released in December 2022.

CVE-2022-42905 is a buffer over-read vulnerability found in wolfSSL versions 5.5.1 and earlier, and could result in exploitable crashes (but only if callback functions are enabled).

It was discovered and reported by Lucca Hirschi and Steve Kremer from LORIA, Inria (the French Institute for Research in Digital Science and Technology) and Max Ammann, a security engineer interning with Trail of Bits. It has been patched in wolfSSL version 5.5.2, released in October 2022.

Fuzzing cryptographic libraries to flag security flaws

In both cases, the researchers used fuzzing to find the flaws.

“Computer software is becoming more complex. So, it is almost impossible to perform a complete source code review with reasonable coverage. For this reason, modern fuzzing methods are used to discover vulnerabilities,” Deutsche Telekom’s security evaluators explained.

They fuzzed the MatrixSSL library with code coverage-guided fuzzers AFL and libFuzzer, and the vulnerability was found with AddressSanitizer, a tool for detecting memory errors. (Using those same tools, several years ago Hörr unearthed another buffer overflow in wolfSSL. He also developed the Fast Automated Software Testing framework for TLS libraries, combining the strengths of various fuzzing tools.)

“Code coverage based fuzzing combined with the AddressSanitizer is a powerful method to discover e.g., buffer overflows. With increasingly complex source codes, it is a resource-efficient alternative to source code reviews, because this fuzzing approach can be done mainly automatically. As there exist many approaches for fuzzing, it is the art of fuzzing to find the best approach,” Hörr and Ibrahim noted.

Ammann and his fellow researchers used a new protocol fuzzer called tlspuffin to automatically discover CVE-2022-42905 and three other vulnerabilities.

“Tlspuffin is a fuzzer inspired by formal protocol verification. Initially developed as part of my internship at LORIA, INRIA, France, it is especially targeted against cryptographic protocols like TLS or SSH,” he explained.

They used the fuzzer not only to discover new vulnerabilities in wolfSSL, but also to rediscover previously flagged logical vulnerabilities (e.g., FREAK) as a way to prove that tlspuffin works.

In an excellent write-up, Ammann went more in-depth about some of the discovered vulnerabilities and how the fuzzer found “weird states” and allowed them to find their source.

“It is challenging to fuzz implementations of cryptographic protocols. Unlike traditional fuzzing of file formats, cryptographic protocols require a specific flow of cryptographic and mutually dependent messages to reach deep protocol states,” he explained.

“Additionally, detecting logical bugs is a challenge on its own. The AddressSanitizer enables security researchers to reliably find memory-related issues. For logical bugs like authentication bypasses or loss of confidentiality no automated detectors exist.”

That’s why they created tlspuffin. Employing the decades-old Dolev–Yao model, which can be used for testing cryptographic protocols, it includes specific modifications so they could successfully fuzz concrete implementations of cryptographic protocols. Tlspuffin’s structure is also based on the LibAFL fuzzer.

“Before my internship at Trail of Bits, tlspuffin already supported fuzzing several versions of OpenSSL (including the version 1.0.1, which is vulnerable to Heartbleed) and LibreSSL,” Ammann noted. Since then, they have:

- Designed an interface that added the capability to fuzz arbitrary protocol libraries and added support for fuzzing wolfSSL

- Added support for fuzzing the SSH protocol, as well as libssh
- Added a security violations oracle that allows for the detection of security issues that do not lead to program crashes (e.g., authentication bypasses or protocol downgrades)
- Made changes that allowed them to more easily validate findings

Tlspuffin can now be used for testing the TLS and SSH protocols, and that integrating a new protocol into tlspuffin is possible, but “takes significant effort and requires an in-depth understanding of the protocol.” It can also be used by developers to write test suites.

16.What’s Happening With Quantum-Safe Cryptography?

by Cliff Saran
https://www.computerweekly.com/news/252529003/Whats-happening-with-quantum-safe-cryptography

Just weeks after US president Joe Biden signed into law the Quantum Computing Cybersecurity Preparedness Act, there are reports that Chinese researchers have cracked RSA 2048 bit encryption.

Given that quantum computers offer the ability to push computational boundaries, such as solving intractable problems such as integer factorisation, which is used for public key encryption, the US government aims to encourage the migration of Federal Government IT systems to quantum-resistant cryptography.

However, last week, a number of news outlets picked up a *Financial Times* story which reported that Chinese researchers claim they can break RSA 2048 encryption using quantum computing.

The researchers published a paper, *Factoring integers with sublinear resources on a superconducting quantum processor*, in which they stated: “We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm. Our study shows great promise in expediting the application of current noisy quantum computers, and paves the way to factor large integers of realistic cryptographic significance.”

They concluded that the pace of development of NISQ devices means they would be able to scale quickly to meet the challenge of cracking RSA 2048 encryption.

In his blog, commenting on the news reports, American cryptographer Bruce Schneier wrote: “I don’t think this will break RSA. Several times a year, the cryptography community received “breakthroughs” from people outside the community. That’s why we created the RSA Factoring Challenge: to force people to provide proof of their claims. In general, the smart bet is on the new techniques not working. But someday, that bet will be wrong. Is it today? Probably not. But it could be. We’re in the worst possible position right now: we don’t have the facts to know. Someone needs to implement the quantum algorithm and see.”

Other security experts have dismissed the claim, describing it as “Chinese propaganda”.

Since 2016, the US National Institute of Standards and Technology (NIST), has been looking to develop a new standard for post quantum cryptography (PQC). In October last year, it announced that the PQC standardisation process would be continuing with a fourth round of submissions.

Discussing the evolution of quantum computers and the potential for them to reach a point where they would be able to crack public key encryption, Daniel Shiu, chief cryptographer at Arqit, said that in the short term, quantum computers will remain inadequate. But, he said: “When you start talking longer term, it’s a question of risk appetite.”

For instance, if there is a 1% chance in the next three years that a public key cracking quantum computing would exist, then that will influence organisations’ risk exposure. Given that NIST began its quest for PQC way back in 2016, and seven years on, it is still looking for submissions, Shiu said the industry is starting to feel jumpy.

“The whole process has taken longer than everybody was hoping,” he said. “There are big maturity and migration concerns, and another part of NIST, the Cyber Centre of Excellence, is doing a migration study where the experts are talking about decades that might be needed to fully update internet public key cryptography.”

Quantum-safe systems

The industry has also been focused on developing quantum-safe systems. Last year, IBM claimed that its newly introduced z16 system was the industry’s first of that description. It said the z16 is able to protect data against future threats that could evolve with advances in quantum computing, and that it uses “lattice-based cryptography”, an approach for constructing security primitives that helps protect data and systems against current and future threats.

The firm said the new hardware provides secure boot, which, when combined with quantum-safe cryptography, can help businesses tackle threats such as “harvest now, decrypt later” attacks, which lead to extortion, loss of intellectual property and disclosure of other sensitive data.

For Shiu, public key encryption, like RSA, represents a pre-internet way to verify the authenticity of a user, and provides public key certificates to support offline validation of credentials.

“We should be moving to a time when we can have much more actively managed trust,” he said. For instance, Kerberos offers a different way to mediate trust based on what Shiu describes as “purely symmetric primitives”. This means it requires a centralised key management server that everybody uses for trust.

But changing a fundamental approach to internet encryption is not something that can easily be rolled out, which is why so much attention is being given to quantum-safe encryption.

17.A 30-Year-Old Cryptographic Challenge Is About To Be Solved

by The Physics arXiv Blog
https://www.discovermagazine.com/technology/a-30-year-old-cryptographic-challenge-is-about-to-be-solved

In 1991, the cybersecurity company, RSA Laboratories in Bedford, Massachusetts published a list of 54 increasingly large numbers that it had created by multiplying two prime numbers together. It then challenged the computer science community to factorize them — to find the original prime numbers in each case. The company even offered cash prizes for some of the solutions.

The challenge was designed to assess state-of-the-art capabilities for factoring numbers. That's important because factoring — or more precisely its difficulty— secures various public key cryptosystems. So advanced factoring capabilities make these cryptosystems less secure.

The challenge ended in 2007 but even today 31 of these **RSA numbers** remain unfactored. The largest is RSA-2048, so-called because of the number of bits required to represent it.

It would be easy to think that progress in factoring numbers must have stalled. But behind the scenes a revolution has been brewing in the form of increasingly capable quantum computers, which are much better at factoring than conventional machines.

For the moment, these machines are not powerful enough to outperform the most powerful conventional computers. And that raises the question of when they will be.

Quantum Algorithm

Today we get an answer thanks to the work of Bao Yan at the State Key Laboratory of Mathematical Engineering and Advanced Computing in China and colleagues who have developed a way to dramatically boost the power of quantum algorithms capable of factoring numbers.

They use their approach to increase the size of the largest number ever factored by a quantum computer. And they say their work paves the way for quantum computers to become capable of cracking codes of "cryptographic significance", such as RSA-2048.

The security of public key cryptosystems depends on the mathematical process of factoring, the reverse of multiplication. The interesting feature of multiplication and factoring is that even though they are closely related, they are vastly different to perform.

Multiplying two prime numbers together to get a bigger number is easy. But starting with the bigger number and working out which primes are factors is hard. In fact, the difficulty increases exponentially with the size of the number, and it is straightforward to make a number so big that a classical computer would need the lifetime of the universe to find its factors.

That's what makes public key cryptosystems so secure — they're not perfect but a conventional computer would need the lifetime of the universe to crack them.

This thinking changed in 1994, when the American mathematician Peter Shor came up with a quantum algorithm that could factor numbers much more quickly than a conventional algorithm. In one foul swoop, Shor's work raised the prospect that any public key cryptosystem could be cracked by a quantum computer in future.

The promise of Shor's algorithm has been a major driving force in the development of quantum computers. But implementing it has turned out to be tricky because it requires quantum computers significantly more powerful than any that are available.

The largest number factored by a quantum computer using Shor's algorithm is just 21. Other approaches have been more successful but nowhere near powerful enough to tackle the RSA numbers. "The largest integer factored by a general method in a real physical system is 249919," say Bao and co.

This a number that can be described in 18-bits. However, modern public key cryptosystems depend on significantly bigger numbers that can be described in 2048 bits or more. That's why these cryptosystems look safe from this kind of attack, but an important question is how long it will be before quantum computers can tackle them too.

Quantum-Classical Hybrid

The breakthrough that Bao and co have made is to speed up an alternative approach to Shor's algorithm, called Schnorr's algorithm (sic). This is a classical algorithm consisting of several steps that each take time to solve.

Bao and co's approach is to use a quantum optimization algorithm to speed up the most time-consuming step. This quantum-classical hybrid approach has the effect of dramatically speeding up the factoring process but with a less powerful quantum computer than is necessary for Shor's algorithm.

The results are impressive. Bao and co have used their approach to factor the 48-bit number 261980999226229 using a superconducting quantum computer with just ten qubits. This is "the largest integer factored by a general method in a real quantum device," say Bao and co.

All this means the prospects for factoring even larger numbers are good. Bao and co calculate that their approach could factor RSA-2048 using a quantum computer with 372 qubits.

"Such a scale of quantum resources is most likely to be achieved in the near future," they say. Indeed, IBM recently unveiled **a quantum computer with 433 qubits**.

There is an important caveat, however. It's not just the number of qubits that determines the capability of a quantum computer but it's error rate and at the moment, quantum computers are too error prone to make larger calculations profitable.

Nevertheless, Bao and co's is interesting work suggesting that the RSA numbers are likely to fall like ten pins in the near future. It's taken more than 30 years, but the RSA Factoring Challenge could finally be close to being solved.

The implications are obvious for the security of public key encryption systems, which are still widely used. Cryptographers have had plenty of time since Shor's announcement to come up with more secure ways to send messages. Whether they have succeeded should shortly be revealed.

18.The Optical Fiber That Keeps Data Safe Even After Being Twisted Or Bent

by University of Bath
https://www.sciencedaily.com/releases/2023/01/230110150806.htm

Optical fibres are the backbone of our modern information networks. From long-range communication over the internet to high-speed information transfer within data centres and stock exchanges, optical fibre remains critical in our globalised world.

Fibre networks are not, however, structurally perfect, and information transfer can be compromised when things go wrong. Tßo address this problem, physicists at the University of Bath in the UK have developed a new kind of fibre designed to enhance the robustness of networks. This robustness could prove to be especially important in the coming age of quantum networks.

The team has fabricated optical fibres (the flexible glass channels through which information is sent) that can protect light (the medium through which data is transmitted) using the mathematics of topology. Best of all, these modified fibres are easily scalable, meaning the structure of each fibre can be preserved over thousands of kilometres.

The Bath study is published in the latest issue of *Science Advances*.

Protecting light against disorder

At its simplest, optical fibre, which typically has a diameter of 125 µm (similar to a thick strand of hair) comprises a core of solid glass surrounded by cladding. Light travels through the core, where it bounces along as though reflecting off a mirror.

However, the pathway taken by an optical fibre as it crisscrosses the landscape is rarely straight and undisturbed: turns, loops, and bends are the norm. Distortions in the fibre can cause information to degrade as it moves between sender and receiver. "The challenge was to build a network that takes robustness into account," said Physics PhD student Nathan Roberts, who led the research.

"Whenever you fabricate a fibre-optic cable, small variations in the physical structure of the fibre are inevitably present. When deployed in a network, the fibre can also get twisted and bent. One way to counter these variations and defects is to ensure the fibre design process includes a real focus on robustness. This is where we found the ideas of topology useful."

To design this new fibre, the Bath team used topology, which is the mathematical study of quantities that remain unchanged despite continuous distortions to the geometry. Its principles are already applied to many areas of physics research. By connecting physical phenomena to unchanging numbers, the destructive effects of a disordered environment can be avoided.

The fibre designed by the Bath team deploys topological ideas by including several light-guiding cores in a fibre, linked together in a spiral. Light can hop between these cores but becomes trapped within the edge thanks to the topological design. These edge states are protected against disorder in the structure.

Bath physicist Dr Anton Souslov, who co-authored the study as theory lead, said: "Using our fibre, light is less influenced by environmental disorder than it would be in an equivalent system lacking topological design.

"By adopting optical fibres with topological design, researchers will have the tools to pre-empt and forestall signal-degrading effects by building inherently robust photonic systems."

Theory meets practical expertise

Bath physicist Dr Peter Mosley, who co-authored the study as experimental lead, said: "Previously, scientists have applied the complex mathematics of topology to light, but here at the University of Bath we have lots of experience physically making optical fibres, so we put the mathematics together with our expertise to create topological fibre."

The team, which also includes PhD student Guido Baardink and Dr Josh Nunn from the Department of Physics, are now looking for industry partners to develop their concept further.

"We are really keen to help people build robust communication networks and we are ready for the next phase of this work," said Dr Souslov.

Mr Roberts added: "We have shown that you can make kilometres of topological fibre wound around a spool. We envision a quantum internet where information will be transmitted robustly across continents using topological principles."

He also pointed out that this research has implications that go beyond communications networks. He said: "Fibre development is not only a technological challenge, but also an exciting scientific field in its own right.

"Understanding how to engineer optical fibre has led to light sources from bright 'supercontinuum' that spans the entire visible spectrum right down to quantum light sources that produce individual photons -- single particles of light."

The future is quantum

Quantum networks are widely expected to play an important technological role in years to come. Quantum technologies have the capacity to store and process information in more powerful ways than 'classical' computers can today, as well as sending messages securely across global networks without any chance of eavesdropping.

But the quantum states of light that transmit information are easily impacted by their environment and finding a way to protect them is a major challenge. This work may be a step towards maintaining quantum information in fibre optics using topological design.

19.Do Not Miss Quantum Computing Wave In 2023

by Nancy Liu
https://www.sdxcentral.com/articles/interview/dell-cto-do-not-miss-quantum-computing-wave-in-2023/2023/01/

Quantum computing is one of the long-term trends that CIOs should take action on in 2023, otherwise "you will miss this technology wave," Dell Technologies Global CTO John Roese argued.

Roese saw patterns forming this year "where we're starting to see some very long trends culminating with something that needs to be done." For CIOs and IT decision-makers, "it's not okay to just be aware anymore, there are certain things that you actually have to act on," he told SDxCentral.

And quantum computing is a good example. This year, organizations should invest in quantum talent, simulations, and security.

Roese noted industrial quantum computing use cases started to emerge two years ago, including battery development, material science, drug discovery, and seismic research. "We have hundreds of examples where people have done the early work to figure out how they would apply quantum mathematics to solve some really hard problems that would make specific industries better."

Additionally, quantum computing tools are available for users to explore the technology and start to learn the necessary programming languages and logic.

To this end, Dell released a hybrid classical-quantum computing package that offers a quantum emulation platform and access to IonQ's quantum computers that can enable both on-premise and cloud-based quantum acceleration last November.

“In almost every industry, we can find examples where people know what they’re going to use a quantum computer for, and then if they can apply it to these problems, mostly optimization problems, they would get an advantage and they’re starting to experiment,” Roese said.

That’s why he recommends organizations build a team or identify a point person for quantum computing implementation.

“It turns out that 2023 is the year that for the first time, most enterprises are going to be able to start to deploy quantum-shaped protocols,” Roese said.

“Investing in quantum simulation and enabling your data science and artificial intelligence (AI) teams to learn the new languages and capability of quantum is critical in 2023,” he wrote in a post.

Determine Quantum-Safe Crypto Risks

To earn a better position for quantum computing, organizations should also draw a clear picture for post-quantum cryptography, Roese noted.

“With the rise of quantum computing comes the need to better understand post-quantum cryptography, the development of cryptographic systems for classical computers that are able to prevent attacks launched by quantum computers,” he warned. “Bad actors globally are actively trying to capture and archive encrypted traffic on the assumption that sufficiently powerful quantum computers will eventually be able to decrypt that data.”

To mitigate those risks, organizations can identify their cryptography inventory and catalog their crypto assets, and then assess their high-risk public interfaces including identifying which encrypted data is most exposed to the public networks — especially those in the hybrid and multi-cloud environments, according to Roese.

Last year, the National Institute of Standards and Technology (NIST) selected the first few viable post-quantum algorithms, “and in 2023 these tools will start to emerge,” he noted. “Over time they will be needed everywhere, but in 2023, knowing where to use them first is a critical step.”

20.Cybersecurity Trends For 2023: How To Protect Your Organization From Attackers In A Recessive Economy

by Megha Kalsi, Nate Morin, David Stanton
https://insights.alixpartners.com/post/102i4qz/cybersecurity-trends-for-2023-how-to-protect-your-organization-from-attackers-in

Doing More With Less: It's The New Shift For Cybersecurity. Driven By A Looming Recession And Increased Management Scrutiny Around Expenses.

But What Does This Look Like In Practice? How Do Cybersecurity Teams Keep Pace With Threats

And Attackers Even As Spending Flatlines? Here Is A Look At 2022 Trends, Some 2023 Predictions, And Recommendations On How Organizations Can Still Protect Themselves While Maintaining Flat Security Budgets. 2022

Cybersecurity Trends Recap

In 2022, Several Key Cybersecurity Trends Were Top-Of-Mind For Organizations. The Increased Prevalence Of Ransomware Attacks, Leveraging Supply Chain Weaknesses And Misconfigurations In Cloud Environments, Remained Popular And Effective With Attackers. As In Previous Years, The Challenge For Defenders Remains Increasing The Attackers' Cost Of Exploitation While Limiting The Blast Radius Of A Successful Compromise. If Your Defenses Raise The Level Of Effort Or Cost Required To Successfully Compromise Your Assets Beyond The Expected Value Of The Compromise The Attacker Hopes To Achieve Through The Attack, It's Likely They'll Move On To Other, More Lucrative Targets.

Again In 2022, Challenges In Hiring Top Security Talent Remained Top Of Mind For Security Leadership, And The Concerns Over Data Privacy Continued To Increase, As Did The Record Data Privacy Fines. Over A Billion Dollars In Gdpr Fines Were Levied In 2022, With Some Individual Companies Facing Fines Of Hundreds Of Millions Of Dollars Each.

2023 Cyber Security Predictions

What Is On The Horizon For 2023? Here Are Eight Up-And-Coming Trends To Watch:

1. **Malicious Use Of Artificial Intelligence In Cybersecurity**

   With The Accelerating Levels Of Maturity In Ai-Fueled Tools, It Is Looking Increasingly Like When And Not If Ai Capabilities Will Be Weaponized By Cybercriminals Looking To Lower The Cost And Increase The Effectiveness Of Their Attacks. Look For An Arms Race In The Coming Years As Ai-Powered Offensive And Defensive Tools Are Increasingly Leveraged By Both Sides.

2. **Ongoing Focus On Ciso Accountability And Insightful Reporting**

   A Recent Study Noted That 70% Of C-Suite Executives Interviewed Agreed That Cybersecurity Should Be A Part Of Every Board Meeting. Thus, Chief Information Security Officers (Cisos) Should Expect An Increased Emphasis On Visibility And Accountability. In Practice, Cisos Should Expect Growing Cybersecurity Awareness And The Requirement To Demonstrate The Impact Of Security Tools And Technologies In Defending Critical Assets Or Avoiding Potential Threats. Boards Expect Accountability And Clear Metrics With Near Real-Time Information On Cyber Threats, Risks To The Business, The Likelihood Of Successful Attacks, And Vulnerability Remediation Progress.

3. **Focus On Clearly Defined Risk Categorization And Risk Tolerances**

   Cisos Will Also Be Expected To Clearly Define Acceptable Cyber Risk Levels And The Metrics Associated With These Levels. Moreover, They Will Be The "Go-To" C-Suite Members Leading The Move From Current Processes To New Operations.

4. **Establishing Justified Cybersecurity Budgets**

   As Budgets Come Under Greater Scrutiny, Security Leaders Will Need To Provide Demonstrable Proof That Current Spending Is Clearly Linked To Reduced Security Risk. In Practice, This Could Include Data Around The Number Of Detected Incidents Versus The Number Of Successful Breaches And, In Turn, The Time, Effort, And Money Saved.

5. **Positioning Of Cybersecurity As A Business Enabler**

   Collaboration Across The Organization Will Be Critical As Companies Look To Move Toward Environments Where Security Is A Business Enabler Rather Than Simply Corporate Compliance Or It Risk Management. Clear Intentions Should Be Made To Achieve Positive Business Outcomes Through Increased Cybersecurity Solution Modernization.

6. **Growing Cyber Security Focus In Automotive And Energy Sectors**

   With Electric Vehicles (Evs) Increasingly Going Mainstream, Automakers And Energy Companies Will Be Under Greater Threat From Nation-State Actors To Obtain Intellectual Property, New Vehicle Features And Layouts, And Other Data That Gives An Automotive Or Energy Company A Competitive Edge. As A Result, There's A Growing Focus On Adaptable And Intelligent Cybersecurity In These Sectors.

7. **Weaponization Of Social Media Platforms**

   Social Media Security Issues Are On Their Way Up In 2023. According To A Study Conducted By Vmware In 2022, 60% Of Security Professionals Said They Spotted The Use Of "Deepfakes" — Legitimate-Looking Images Often Lifted From Social Media Profiles That Help Malicious Actors Carry Out Fraud Via Social Engineering.

8. **Unaffordable And Low Payout Cyber Insurance**

   Cyber Insurance Is Getting More Expensive Even As The Probability Of Having A Pay Out In The Event Of An Incident Is Decreasing. As Noted By Dark Reading, For Example, Cyber Insurance Providers Such As Lloyd's Of London Recently Announced That Their Policies Would Exclude Coverage For State-Sponsored Cyberattacks.

Recommendations For Cybersecurity Success In 2023

With Budgets Flatlining As The Visibility Of Cyber Issues And Expectations Increase, Where Does This Leave Security Teams? While There's No Silver Bullet To Solve Cybersecurity Issues At The Lowest Cost Possible, There Are Opportunities For Organizations To Minimize The Risk To Their Systems And Data While Also Optimizing Their Security Spend.

Begin The New Year With A Fresh Look At Your Security Risk Tolerance. Does The Current Model Still Accurately Reflect The Top Security Risks To The Business, And Is Your Security Program Still Focused On Mitigating And Measuring Any Remaining Risks? If Gaps Are Found, Are Your Security Program Priorities And Spending For 2023 Targeted Toward Those Gaps, And If Not, Why Not?

Security Leaders Should Also Revisit Their Security Program Organizational Structure To Reassess Each Team’s Function And The Responsibilities Of All The Roles Across Their Organization. Reevaluate Whether The Current Structure Is Sustainable And Can Address Risk Tolerance Needs, Tackle Upcoming Projects, Address Security Ad-Hoc Requests, And Perform Daily Operations On A Reduced Budget Or The Current Budget. Further, Consider The Usage Of Managed Security Service Providers (Mssp) Or Third-Party Contracts To Offset Costs Or Provide Expert Insights On Areas Lacking Security Maturity (E.G., Data Security, Endpoint Security, Network Security, Cloud Security, Etc.).

Today, It Is More Critical Than Ever To Keep Breaking Down Silos. While This Has Been A Priority For Many Companies Over The Past Few Years, Companies Can't Afford To Take Their Foot Off The Gas Now. By Implementing Businesswide, Cloud-Based Policies And Procedures, It's Possible To Create A

Security-By-Design Framework That Embeds Protections Into Key Functions.

Finally, It's Worth Evaluating Where You Could Save Money On Cyber Security Without Compromising Overall Protection. Potential Areas For Improved Cost Management Include:

1. **Streamlining Security Tools**

   The Fewer Security Tools You Use, The Lower The Overall Cost And The Smaller The Risk Of Something Slipping Through The Cracks. More Tools Sometimes Result In Too Much Data Or Even Conflicting Data That Needs To Be Rationalized. Ensure Any New Tools Fill A Specific Need That Maps To Gaps In Your Coverage Model From Whatever Frameworks You've Chosen To Support Your Risk Tolerance.

2. **Examining Current Mssp (Managed Security Service Provider) Capabilities**

   With More Than 10,000 Mssps In Operation, It Is Worth Comparing Current Provider Capabilities And Costs To Other Market Options. Partnering With An Mssp Isn't An All-Or-Nothing Decision. It Could Be As Simple As Receiving Staff Augmentation To Provide 24X7 Coverage Of Critical Events Or As Broad As Fully Outsourcing The Specific Security Product Choice, Deployment, And Operations As Many Are Considering In The Endpoint Detection And Response (Edr) Space.

3. **Working Backward To Move Forward**

   As Attack Vectors Evolve, New Security Tools Will Be Required. To Keep Spending Under Control, Start From What You Have And Work Backward To Pinpoint Areas Where Current Tools Do Not Cover Critical Gaps. Invest The Savings In Further Modernizing, Standardizing, And Securing Your Cloud-Based Workloads. Greater Degrees Of Solution Standardization And Automation Can Drastically Reduce Configuration Errors And Vulnerabilities And, Over Time, Reduce Operational Costs And Risk.

4. **Re-Evaluating Cybersecurity Insurance Policies**

   Organizations Need To Constantly Evaluate Their Cyber Insurance's Efficacy And Cost To Ensure It Is Filling A Critical Need And Offers Substantial Value. If You Are Paying Tens Of Thousands Per Month For Coverage With A Low Likelihood Of A Payout In The Event Of A Covered Attack, It May Be Time To Rethink Your Current Policy Or Provider. Some Organizations Are Even Considering Reducing The Amount Of Cyber Insurance Coverage They Purchase Or Self-Insuring, Given The Changes In The Insurance Market.

What Is The Bottom Line? Budgets Aren't Getting Bigger, But Business Leaders Expect Cybersecurity To Increasingly Become A Business Enabler In 2023. To Do More With Less, Teams Need To Focus On The Basics, Evaluate Their Insurance, Break Down Silos And Look For Ways To Reduce Spending Without Sacrificing Security.

21.Will Quantum Computers Break RSA Encryption In 2023?

by Stan Kaminsky
https://www.kaspersky.com/blog/quantum-computers-and-rsa-2023/46733/

In the final days of 2022, the IT community was rather stirred by a study presented by a group of Chinese scientists. It claimed that in the nearest future it will be possible to crack the RSA crypto algorithm with a key length of 2048 bits – which is fundamental for the operation of internet protocols – by skillfully combining classical and quantum computing. So how real is this threat? Let's figure it out.

Quantum basics

The theoretical ability of a quantum computer to perform ultra-fast factorization of giant integers and thus match keys for a number of asymmetric crypto-algorithms – including RSA encryption – has long been known. Our blog post explains in detail what a quantum computer is, how it works, and why it's so difficult to build. So far, all experts have agreed that a quantum computer large enough to crack RSA would probably be built no sooner than around a few dozen decades. To factorize an integer 2048 bits long, which is usually used as an RSA key, the Shor algorithm needs to be run on a quantum computer with millions of qubits (quantum bits). That is, it's not a matter of the nearest future, since the best quantum computers today work at 300-400 qubits — and this is after decades of research.

But the future problem has already been actively thought about, and security experts are already calling for adoption of post-quantum cryptography; that is, algorithms that are resistant to hacking with a quantum computer. There seemed to be a decade or more for a smooth transition, so the news that RSA-2048 might fall as early as in 2023 came as a bolt from the blue.

News from China

Chinese researchers have been able to factor a 48-bit key on a 10-qubit quantum computer. And they calculated that it's possible to scale their algorithm for use with 2048-bit keys using a quantum computer with only 372 qubits. But such a computer already exists today, at IBM for example, so the need to one day replace crypto-systems throughout the internet suddenly ceased being something so far in the future that it wasn't really thought about seriously. A breakthrough has been promised by combining the Schnorr algorithm (not to be confused with the aforementioned Shor algorithm) with an additional quantum approximate optimization algorithm (QAOA) step.

Schnorr's algorithm is used for supposedly more efficient factorization of integers using classical computation. The Chinese group proposes to apply quantum optimization at the most computationally intensive stage of its work.

Open questions

Schnorr's algorithm was met by the mathematical community with certain skepticism. The author's claim that "this will destroy the RSA cryptosystem" in the description of the study was subjected to scrutiny and didn't stand up. For example, famous cryptographer Bruce Schneier said that it "works well with smaller moduli — around the same order as ones the Chinese group has tested — but falls apart at larger sizes." And no one has succeeded in proving that this algorithm is scalable in practice.

Applying quantum optimization to the "heaviest" part of the algorithm seems like a good idea, but quantum computing experts doubt that QAOA optimization will be effective in solving this computational problem. It's possible to use a quantum computer here, but it will unlikely lead to time savings. The authors of the work themselves carefully mention this dubious moment at the very end of their report, in the conclusion:

- It should be pointed out that the quantum speedup of the algorithm is unclear due to the ambiguous convergence of QAOA.
- …

- Besides, the quantum speedup is unknown, it is still a long way to break RSA quantumly.

Thus, it looks like even if you implement this hybrid algorithm on a classical + quantum system, it will take as long to guess RSA keys as with a regular computer.

The icing on the cake is that in addition to the number of qubits there are other important parameters of a quantum computer, like levels of interference and errors, and the number of gates. Judging by the combination of required parameters, even the most promising computers of 2023-2024 are probably not suitable for running the Chinese algorithm on the needed scale.

Practical takeaways

While the crypto revolution is once again being delayed, the buzz around this study highlights two security-related challenges. First, when choosing a quantum-resistant algorithm among numerous proposals for a "post-quantum standard", new algebraic approaches – such as the aforementioned Schnorr's algorithm – should be studied scrupulously. Second, we definitely need to raise the priority of projects for the transition to post-quantum cryptography. It will seem like a non-urgent matter only until it's too late…

22.Chinese Researchers' Claimed Quantum Encryption Crack Looks Unlikely

by Thomas Claburn
https://www.theregister.com/2023/01/07/chinese_researchers_claimed_quantum_encryption/

Briefly this week, it appeared that quantum computers might finally be ready to break 2048-bit RSA encryption, but that moment has passed.

The occasion was the publication of an academic paper by no less than two dozen authors affiliated with seven different research institutions in China.

The paper, titled "Factoring integers with sublinear resources on a superconducting quantum processor," suggests that the application of Claus Peter Schnorr's recent factoring algorithm, in conjunction with a quantum approximate optimization algorithm (QAOA), can break asymmetric RSA-2048 encryption using a non-fault tolerant (NISQ, or noisy intermediate scale quantum) quantum computer with only 372 physical quantum bits or qubits.

If true, this would be a significant development because there are already quantum computers that exceed that specification, like IBM's 433-qubit Osprey.

The speculation has been that orders of magnitude more qubits, in conjunction with robust error correction at scale, may allow future quantum computers to run Peter Schor's algorithm – not to be confused with the similarly named Schnorr – quickly, on very large numbers, thereby breaking RSA encryption.

In 2019, researchers published a paper [PDF] claiming that 2048-bit RSA integers could be factored in about eight hours … given a quantum computer with 20 million noisy qubits (meaning without the overhead of error correction and the like).

That's a future the National Security Agency has been planning for since 2015, when it started public work on developing quantum-resistant encryption algorithms.

No one is quite sure when, or whether, that day will arrive. When we considered quantum crypto-cracking in 2019, University of Chicago computer science professor Diana Franklin suggested, "It is possible that Shor's algorithm could be implemented in the next 15 years," while allowing predictions of this sort are notoriously difficult to get right.

Nonetheless, the quantum gold rush is on. The US and China, along with Europe, the UK, and other countries in Asia are all working to lead the nascent quantum computing industry and to avoid being caught flat-footed if a breakthrough occurs.

Let's look at the facts

Public (asymmetric) key cryptography secures the financial system via digital signatures and certificates. Being able to forge those with a sufficiently capable quantum system would be problematic to say the least. Symmetric cryptographic algorithms, like AES-256, are considered to be more resistant to quantum computers, so the application of Grover's algorithm [PDF] in a quantum system isn't expected to alter the cryptographic landscape.

The paper from 24 researchers in China might have remained a matter for those well-versed in advanced mathematics, cryptography, and quantum computing – a fairly small set of people – but for the fact that it got noticed by cryptographer Bruce Schneier.

"This is something to take seriously," he wrote in his blog on January 3rd, 2023. "It might not be correct, but it's not obviously wrong."

Schneier did not take a position on the paper, but the following day The Financial Times took notice in an article titled, "Chinese researchers claim to find way to break encryption using quantum computers."

Evidently they haven't.

Late that day, on January 4, Scott Aaronson, chair of computer science at The University of Texas at Austin, and director of its Quantum Information Center, offered a rebuttal with a succinct three word review of the paper: "No. Just No."

Aaronson, among the more credible voices on such matters, hangs the researchers with their own caveat: "It should be pointed out that the quantum speedup of the algorithm is unclear due to the ambiguous convergence of QAOA," they wrote in their paper.

That's a vast understatement, Aarsonson argues, because it has yet to be demonstrated that Schnorr's algorithm, even with QAOA, will work faster on a quantum device than a classical computer. And if a current laptop could break RSA, doing so on a quantum computer would be unnecessary.

"All told, this is one of the most actively misleading quantum computing papers I've seen in 25 years, and I've seen … many," he wrote.

23.Have Chinese Scientists Really Cracked RSA Encryption With A Quantum Comput-

er?

by Ryan Morrison
https://techmonitor.ai/hardware/quantum-encryption-rsa-cryptography

Chinese researchers have surprised the security community by claiming to have cracked low-level RSA encryption – the standard encryption method used for secure data transmissions around the world – using a hybrid of a quantum and classical computer. The scientists say their method could be used to defeat advanced 2048-bit RSA encryption using a 372-qubit quantum computer, something which would have major security implications.

Such a breakthrough, which could potentially leave corporate networks – and the entire internet – at the mercy of cybercriminals, was thought to be years away, and post-quantum cryptography experts are sceptical about the significance of the claims. They told *Tech Monitor* the methods described "won't scale as expected" and that public-key cryptography is secure "for now".

The quantum computing threat to encryption

There is a race against both time – and the rapidly developing quantum computing industry – to replace RSA and other standard cryptography solutions with post-quantum cryptography which could withstand attacks from such machines. These have the potential to be much more powerful than their classical counterparts, meaning they could break existing encryption methods in a matter of hours or days.

The assumption that quantum computers will eventually break RSA encryption stems from an algorithm published by mathematician Peter Shor in 1994 that has the potential to break most current cryptographic systems, including RSA, in a short amount of time. But it requires a large, stable quantum computer with millions of qubits [the unit of quantum compute power] to work, something which is likely a decade or more away from being a reality. The most advanced machine currently is IBM's Osprey, which is due to come online later this year and will have 433 qubits.

So the new pre-print paper from researchers at the State Key Laboratory of Mathematical Engineering and Advanced Computing in Zhengzhou, China, has raised eyebrows. It proposes a different algorithm that could crack 2048-bit RSA with a low-level quantum computer.

It is based on a solution proposed by German mathematician Claus-Peter Schnorr, who wrote in 2022 that you could factor large numbers in a more efficient way, breaking the RSA code and doing so with a classical computer.

Classical quantum hybrid used to crack RSA encryption

Schnorr's technique couldn't be scaled to work with a regular computer, but the new paper claims to fill in the gap by using a quantum machine to take over part of the calculation, handing the rest to a classical computer. The team say they cracked 48-bit RSA using a 10-qubit quantum computer-based hybrid system and could do the same for 2048-bit if they had access to a quantum computer with at least 372 qubits.

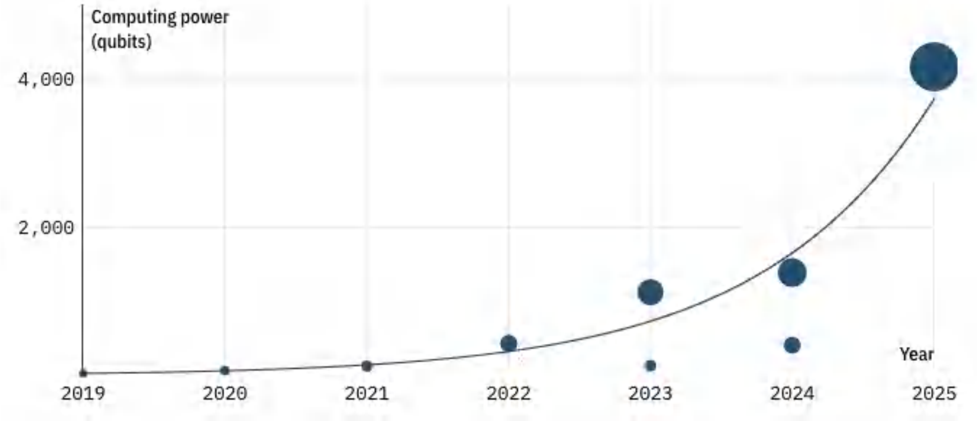
The work reflects a greater drive towards hybrid quantum/classical solutions that includes work by the Riken Institute in Japan to connect a quantum computer to its own supercomputer, Fugaku.

Despite the claims in the paper holding a lot of promise, and hybrid solutions likely representing the short-term future of quantum computing, Ali Kaafarani, CEO and founder of post-quantum cryptography leader PQShield, said the Chinese team “failed to deliver on the promise” of its research.

“Unfortunately, both the classical and the quantum subroutines of the proposed algorithm have serious scalability issues, and in addition, the paper only focuses on the number of qubits – totally ignoring the running time of the proposed algorithm,” he says.

IBM's combined quantum computing power growth is accelerating

IBM quantum computing chips, existing or in the pipeline (2019-2025)



*Values for the Flamingo (2024) and Kookaburra (2025) chips are lower-end estimates

At the end of the paper, the team warns that “quantum speed-up of the algorithm is unclear due to the ambiguous convergence of QAOA”, which is the quantum subroutine used to solve the prime numbers and crack RSA. This suggests there is little evidence it will actually scale as predicted, Kaafarani explains.

“Note that this work is unrelated to Shor’s algorithm,” he says. “That is known to break RSA in polynomial time, and is the main reason for switching to post-quantum cryptography.”

Polynomial time refers to the amount of time it takes for an algorithm to solve a problem, and is generally considered to be good running time for a given algorithm, meaning it can scale to large input sizes without taking an impractically long time to complete. Want to crack RSA encryption? You might need millions of years

Speaking to the *FT*, Shor said that the paper failed to address how fast the algorithm would run to crack 2048-bit RSA, leaving open the prospect it would not be able to complete the work in any reasonable time, and suggesting it “could still take millions of years” as it would with a classical computer.

“In the absence of any analysis showing that it will be faster, I suspect that the most likely scenario is that it’s not much of an improvement,” he said.

Bruce Schneier, security research and technologist, wrote a blog post on the findings, warning that even if this doesn't scale "it is something to take seriously" and that "in general, the smart bet is on the new techniques not working. But someday, that bet will be wrong. Is it today? Probably not. But it could be.”

“We’re in the worst possible position right now: we don’t have the facts to know," Schneier added. "Someone needs to implement the quantum algorithm and see.”

The moment a quantum computer breaks RSA and other cryptography solutions is known as Q-Day among researchers, and it could be anything from a few years to decades away. The significant advantage this would give to a government was cited by some experts as a reason to doubt the Chinese researchers, arguing that if they really had cracked 2048-bit RSA, the Chinese government would have classified the research.

Tim Callan, chief experience officer at security company Sectigo, says it is worth considering the risk of "harvest now decrypt later" as a method that could break RSA-encrypted data in a matter of months or even a few years, as despite not being as rapid as Shor's algorithm, it would open many sensitive secrets to potential exposure. "Think about things like state secrets or manufacturing processes as the information to worry about," Callan says.

"To prepare for RSA decryption, whether it occurs in the short or the long term, organisations must begin researching how hybrid certificates will eventually enable their agility to transition between RSA and either ECC (elliptic-curve cryptography) or quantum-safe algorithms, depending on the circumstances."

He adds: "In the event that quantum decryption becomes possible, implementing hybrid certificates provides a much-needed bridge for organisations to switch hard-coded systems from one encryption algorithm to another."

24.Who Are The Early Adopters Of New Quantum-Secure Cryptography?

by Ali El Kaafarani
https://www.forbes.com/sites/forbestechcouncil/2023/01/06/who-are-the-early-adopters-of-new-quantum-secure-cryptography/?sh=2816b83b791f

From seatbelts to GDPR, any time new standards are introduced, their adoption naturally comes with a certain amount of industry upheaval—and that's exactly what we're now seeing with post-quantum cryptography (PQC).

In July 2022, the U.S. National Institute of Standards and Technology (NIST) published draft standards for PQC, meaning those that want to upgrade their cryptography to manage a new generation of quantum threats need to start doing so.

The U.S. government has requested that all of its departments and partners must transition to the new PQC standards by 2035. Where the U.S. government leads, others inevitably follow. Smart businesses should be setting out their transition pipelines now or risk leaving themselves exposed to cyber, regulatory and commercial risk. Given the scale of the challenge ahead, this is now a boardroom issue—not just a specialist concern for a handful of security professionals.

Already, a few early adopters are leading the pack, but who are they, and why are they taking the quantum threat so seriously?

1. Companies Designing Connected Products With Long Lifecycles

With new cryptography standards due to be implemented by the end of 2023, any designers working on a secure product with a shelf life of five years or more should be asking vendors about how to incorporate post-quantum cryptography. Otherwise, they are designed for obsolescence.

Connected vehicles are a good example. The cars being designed today are more complex than ever, with software controlling everything from airbags to new features like autonomous driving. New vehicles rolling off the assembly line in 2023 will still be on our roads in 15 to 20 years time, which means they will be vulnerable to quantum attack unless manufacturers build in post-quantum cryptography.

Forward-thinking product designers are already mapping their exposure to the quantum threat. This process starts by assessing the encryption embedded in their hardware, as this is typically more costly and time-consuming than overhauling the encryption protecting their software.

2. Components Manufacturers

For those who sit high in the supply chain, providing quantum-safe products is becoming ever more of a competitive advantage. As we've already seen, quantum security plays well with companies designing for the long term or who want their product to stand out from the pack.

We have already seen semiconductor manufacturers like Microchip assessing quantum encryption and companies like IBM developing quantum-secure HSMs. A growing number of wired and wireless networking businesses are also part of the wave of suppliers getting ahead of this trend.

Over time, components manufacturers will play an important and strategic role in facilitating the global transition to quantum security. It's, therefore, reassuring to see them among the earliest adopters of PQC.

3. Highly Regulated Businesses

Sectors like finance and healthcare are already under strict requirements when it comes to securing confidential data, storing it safely and protecting it in transit. As a result, it's natural that this sector includes a number of early PQC adopters.

Mastercard, for example, recently announced a new credit card protected by post-quantum cryptography—one of the first of its kind and a great example for the industry.

Of course, much more is needed before true quantum security is achieved here. In a single transaction, data is vulnerable whenever it passes between systems and devices, so protecting a credit card alone is like changing the lock on a house that has no walls. To defend against the quantum threat, every touchpoint must be protected. Financial institutions need to be mapping their exposure and building coherent plans to upgrade their encryption across the board.

Healthcare, meanwhile, is already a significant target for threat actors looking to harvest sensitive information. Providers in this sector are also acutely aware of the moral and reputational responsibility involved in safeguarding personally identifying patient data, so where they can, they are already thinking about taking steps to explore PQC solutions.

For national health systems like the U.K.'s NHS, this is a slow and complex undertaking that requires input from multiple departments and suppliers. But for the most innovative healthcare players, there are significant incentives for taking PQC seriously.

4. Defense, Critical Infrastructure And Highly Secure Businesses

Recent U.S. government instructions are clear: If your business plans to hold government contracts, then you must secure your digital assets from the emerging quantum threat.

In response, the defense industry is one of the most obvious sectors where PQC will be strategically essential and is already starting to be rolled out. Companies operating in this sector routinely handle high-value strategic assets and interact with sensitive systems, making data security mission-critical. Quantum security is a critical part of their value proposition.

Telecoms and utilities companies have also been spurred into action by the White House. In their case, quantum computers threaten to expose critical infrastructure to an attack, with potentially devastating consequences. That's why companies like Vodafone are convening post-quantum taskforces, working on solutions to the quantum threat and planning a route to quantum security.

Secure communications apps are also vulnerable. These are often used by journalists, whistleblowers and political parties to exchange sensitive information, so the data exchanged via these apps can be particularly damaging in the hands of bad actors. PQShield recently shared guidance with the Signal Foundation for how to address this and bring end-to-end encrypted messaging into the PQC era. These recommendations, along with wider efforts by telecommunications networks to protect their infrastructure, will be crucial to protecting our data in transit.

The Journey Ahead

We are in a window where offering PQC solutions can bring a competitive advantage, but this will close quickly. Cryptographic standards are changing, and the reality is that, sooner or later, all businesses will need to adopt post-quantum cryptography.

For now, though, early adopters are playing an important role in drawing attention to the quantum threat, pushing PQC research and implementation forward and setting the bar for everyone else.

25.QuSecure's Leading Post-Quantum Cybersecurity Solution Wins 2022 Cybersecured Award For Quantum Computing

by Dan Spalding
https://www.businesswire.com/news/home/20230105005421/en/

QuSecure, a leader in post-quantum cybersecurity (PQC), today announced that its industry-leading PQC solution QuProtect™ won the 2022 CyberSecured Award, as announced in December 2022 by 1105 Media's *Security Today* brand, the leading industry media brand providing technology, education and solutions for security professionals. QuProtect, the industry's first and only end-to-end PQC software-based solution uniquely designed to protect encrypted communications and data with quantum-resilience using quantum secure channels, won in the Quantum Computing awards category.

"2023 is going to be a very important year for securing the nation's networks with post-quantum cybersecurity protections, and we are pleased to be recognized as the leading solution with this quantum computing award," said Skip Sanzeri, QuSecure Founder and COO. "Our QuProtect solution enables organizations to protect their communications and secure private information as the world accelerates toward a quantum future, including quantum computing's ability to break our current encryption. QuProtect uniquely combines QuSecure's post-quantum technologies providing secure, interoperable cybersecurity to protect networks from today's classical threats and future quantum threats."

Launched in 2020 by 1105 Media's security group, this program focuses on the network and other cybersecurity initiatives. The CyberSecured Awards honor the outstanding product development achievements of manufacturers and suppliers whose products or services are considered particularly noteworthy in the transformation of cybersecurity. Winners of this independently judged contest will be featured on the security industry leading website, securitytoday.com, and will be recognized in CyberSecured e-news.

"Our *Security Today* CyberSecured Awards are closely aligned with the readership of CyberSecured eNews, a monthly digital publication," said Ralph C. Jensen, editor-in-chief of *Security Today* magazine, and CyberSecured eNews. "We are so pleased that many cybersecurity professionals join us to showcase new products and advanced technology. We are aware of the importance that cybersecurity plays in today's society and have updated our website to include more case studies and thought leadership articles. We're excited to be part of this burgeoning industry and plan to broaden our knowledge base to serve our readership by tapping into the vast experience of professionals and organizations."

QuProtect software enables organizations to leverage quantum resilient technology for the first time to help prevent today's cyberattacks, while future-proofing networks and preparing for post-quantum cyberthreats. It provides quantum-resilient cryptography, anytime, anywhere and on any device. QuProtect software uses an end-to-end quantum-security-as-a-service (QSaaS) architecture that addresses the digital ecosystem's most vulnerable aspects, uniquely combining zero-trust, next-generation post-quantum-cryptography, quantum-strength keys, high availability, easy deployment, and active defense into a comprehensive and interoperable cybersecurity suite. The end-to-end approach is designed to protect the entire information lifecycle as data is communicated, used and stored.

The QuProtect solution is the industry's most advanced PQC solution providing quantum-resilience for many of today's critical use cases, including national security, network, IoT, edge devices, and even satellite communications. QuProtect software can be hosted on-premises or via the cloud delivering the most compatible solution to the post-quantum problem, solving today's complex compliance challenges, such as bring-your-own-device (BYOD) and work-from-home policies. An organization can implement PQC across all devices on the network with minimal disruption to existing systems, protecting against current classical and future quantum attacks which could irreparably disrupt industries and infrastructures across government and commercial sectors.

26.TAU Engineers Launching First Israeli Nanosatellite For Communicating From Space

by Judy Siegel-Itzkovich
https://www.jpost.com/science/article-726654

A nanosatellite that was launched into space by a Tel Aviv University team of engineers on Tuesday will pave the way toward quantum communication, a field of applied quantum physics closely related to quantum information processing and transferring data from place to place.

Its most interesting application is protecting information channels against eavesdropping by means of quantum cryptography. This is the first optical ground station in Israel, and one of very few worldwide that can lock onto, track and collect data from a nanosatellite.

This satellite, which comes after the development of two others in less than two years by TAU, represents a "scientific breakthrough, paving the way toward demonstration of optical and quantum communication from space via nanosatellites," according to the researchers at the Center for Nanosatellites at TAU's Fleischman Faculty of Engineering.

"TAU leads Israel's effort to create satellite communication channels based on optical and quantum technologies," according to the researchers, led by the center's Prof. Meir Ariel. "To implement long-distance quantum communication over hundreds of kilometers or more, we need to go into space. TAU-SAT3 is designed to pave the way toward demonstrating quantum communication via a quantum nanosatellite, to be built in the future at TAU."

The university's first two nanosatellites were designed to measure cosmic radiation around the Earth and test various means of protecting the electronic systems installed on satellites from this radiation, he said.

"To this end, the nanosatellites carried special payloads built in collaboration with various scientific institutions, including the SOREQ Nuclear Research Center.

"The third satellite, TAU-SAT3, was the first to be fully designed, developed and built at TAU," Ariel said.

Faculty dean Prof. Noam Eliaz said that "The Faculty of Engineering is proud of the TAUSAT3 nanosatellite's successful launching. The launch is a result of research and development executed by the Nanosatellites Center in collaboration with the QuanTAU Center.

"This nanosatellite forges a number of milestones on our way to achieve quantum communication from space by means of a quantum nanosatellite, which will be built at TAU in the future," he said.

"Recently, we were the sole winners of a tender by Israel's Innovation, Science and Technology Ministry to build and launch a fleet of satellites while making the field of 'New Space' and building nanosatellites accessible to students in the periphery. As of today, our faculty is the leader in this field in Israel and is a focal point for students, schoolchildren, research centers and industry in this field."

Launched to an altitude of 550 km., TAU-SAT3 is expected to orbit the Earth for about five years and carry out several scientific tasks. For the first time, it carries on board batteries made by the Israeli company Epsilor that will provide it with energy for its entire life in orbit. Its main mission will be to communicate with the new optical ground station set up on the roof of the Shenkar Physics Building on the TAU campus.

This is the first optical ground station in Israel, and one of very few worldwide, that can lock onto, track and collect data from a nanosatellite which – when viewed from Earth – is smaller than a single pixel. According to the researchers, this means that it will be technologically possible in the future to build and launch nanosatellites for optical communication at a much lower cost than large satellites.

The satellite will also conduct experiments in satellite communication at very high bit rates and in scenarios where satellite communication channels have been disrupted.

"TAU-SAT3 is a 20-cm. nanosatellite carrying an optical device that is only a few centimeters long," Ariel said. "When the satellite passes over Israel, the device will emit light at various wavelengths, and the telescope of the optical ground station will identify the tiny flash, lock onto it and track it. The nanosatellite will simultaneously send both optical and radio signals back to Earth.

“However, when the optical device turns toward the optical ground station, the antenna will face in a different direction,” he said. “As a result, a significant portion of the data might be lost. The novelty in this project is the ability of the communication systems installed in both the nanosatellite and the ground station to reconstruct the lost data in real time using smart signal processing algorithms developed at TAU.”

PROF. YARON OZ, head of TAU’s Center for Quantum Science and Technology and a former TAU rector, said that “the principles of quantum mechanics enable an unconditionally secure encryption method. Whenever a hostile entity tries to intercept a transmitted message, the message immediately dissipates. Moreover, the interception attempt is detected – unlike current encryption methods, in which interceptions remain undetectable.

“Consequently, eavesdropping-proof quantum communication is today at the forefront of scientific research,” he said. “Governments and giant organizations around the world are involved in a race for quantum encryption capabilities – especially since quantum computers are expected to crack today’s encryption algorithms. It’s an enormous effort – in terms of science, technology and budgets.

“Beyond the encryption of security data, once current encryption methods are cracked by quantum computing, all data will be exposed – including personal medical and financial records, email and WhatsApp messages. This makes quantum encryption highly relevant to protecting everyone’s privacy,” he said.

“Quantum communication is very sensitive to the medium through which it is transmitted, such as optical fibers or the atmosphere. We hope that TAU-SAT3 will for the first time enable communication between an optical ground station and a satellite, taking us a significant step forward with regard to demonstrating reliable quantum communication.”

27.2023 Will See Renewed Focus On Quantum Computing

by Dark Reading Staff
https://www.darkreading.com/tech-trends/2023-will-see-more-focus-on-quantum-computing

2022 was a big year for quantum computing. Over the summer, the National Institute of Standards and Technology (NIST) unveiled four quantum computing algorithms that eventually will be turned into a final quantum computing standard, and governments around the world boosted investments in quantum computing. 2023 may be the year when quantum finally steps into the limelight, with organizations preparing to begin the process of implementing quantum computing technologies into existing systems. It will also be the year to start paying attention to quantum computing-based attacks.

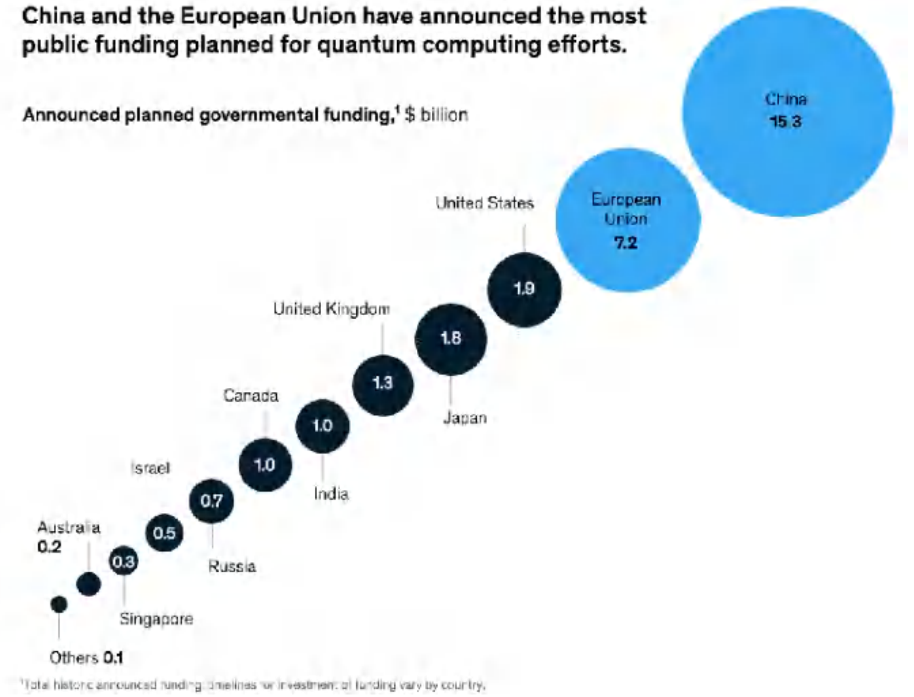
"In 2023, we'll see both the private and public sector's increased awareness around the challenges associated with quantum resilience, and we'll see efforts begin to take hold more significantly to prepare for quantum computing," says CISO (ISC)2 Jon France.

McKinsey recently noted the amount of money different countries have allocated for quantum computing to date. China leads the pack with $15.3 billion in public funds in quantum computing investments. The European Union governments combined have invested $7.2 billion, which dwarfs the US with $1.9 billion.

That doesn't mean the US has been standing still. A key effort — the list of four NIST-approved algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+) — will help organizations future-proof current data security measures against harvest-now/decrypt-later (HNDL) attacks. These attacks refer to adversaries hanging on to encrypted items until a time when quantum computing technology that can decrypt them become available. And last month, US president Joe Biden signed the Quantum Computing Cybersecurity Preparedness Act (HR 7535) into law to give the Office of Management and Budget authority to begin implementing NIST-approved quantum algorithms throughout the executive branch.

The new law highlights the importance of implementing quantum computing technologies into existing systems now, but it doesn't address the necessity of monitoring for threats, says Yudong Cao, co-founder and CTO of Zapata Computing. "We should be actively monitoring the threat by sponsoring cybersecurity research activities into various methods, exact or heuristic, for compromising the current encryption schemes," Cao says.

There is also a lot of investment activity in the private sector, with startups focused on quantum technologies collecting $1.4 billion in funding in 2021 alone, according to McKinsey. Nearly half (49%) of those private investments are in companies in the United States, compared to just 6% in China, the analysts noted.



China and the European Union have announced the most public funding planned for quantum computing efforts.

Announced planned governmental funding,[1] $ billion

[1] Total historic announced funding; timelines for investment of funding vary by country.

"Building cyber resilience in preparation for quantum technology should have been an effort started a decade ago ... but now is the second best time," France says. However, for both private and public-sector organizations, the process of making infrastructure "quantum-resilient" will be a difficult and slow one.

"Much of the encryption infrastructure in communication networks that keeps information safe now is deeply embedded, i.e., certificates, and will take years to transition to quantum resilient algorithms, posing a timeline issue for changeover before the general availability of quantum computing," France says.

In a recent survey by Deloitte, enterprises said that without external pressure — such as regulatory and compliance requirements — they won't be prioritizing quantum security initiatives.

28.Quantum Computing To Become More Accessible

by CXOtoday News Desk
https://www.cxotoday.com/news-analysis/quantum-computing-to-become-more-accessible/

Imagine what it would be to use quantum computing and do so using that desktop that one uses for regular tasks? Well, this ain't science fiction anymore as Quantum Computing Inc (QCI) is all set to manufacture QC optical chips with encryption and authentication at a commercial level that would make the power of quantum computing available to more people.

A report published in SDxCentral quotes QCI chairman and CEO Robert Liscouski as saying that his company's goal and larger roadmap is to add the power of a desktop quantum computer and all its capabilities into a microchip that can get plugged on to a normal PC that quickly goes hybrid and does so pretty quickly and at an affordable price.

Shifting over to commercial usage

The official said QCI would manufacture quantum computing optical chips with encryption, authentication and quantum entanglement distribution capabilities at a commercial level. And the company would then distribute these chips across the board to create a significant uptick in the marketplace for quantum computing.

And that's not all. The company is also seeking out a platform approach for encryption, authentication and quantum entanglement capabilities in order to secure communications, computing and authentication. This would help take on layer encryption with authentication and entanglement distribution. This ensures security of the transport layer and the ability to do peer-to-peer authentication and encryption as well, says Liscouski.

Moving from small scale to large scale

It is not that QCI does not provide these capabilities today. However, this is at a very small scale to be effective in enhancing demand. What the company is now hoping for is to utilize government funding to commercialize these technology capabilities and ramp up manufacturing processes to make the products viable at a lower cost but spread wider.

Last year, QCI had announced plans to construct and operate a quantum nanophotonics tech manufacturing and research center to expand its chip development capabilities. The company is reportedly working on several offers of funding from the federal government, states and even regional-level capital infusion to help finance the project.

In a statement, the company had expressed hope of raising $30 million from incentives that include the CHIPS and Science Act of 2022 which aims to provide over $200 billion over the next decade to fund domestic research and semiconductor manufacture as part of the US government's efforts to compete with Chinese companies.

According to Liscouski, the CHIPS Act offers enough cash for research and development, which is the area that QCI operates in with its photonic quantum chip. Though the company hasn't yet received any funding, they're working with states to put together a package that could potentially present a better funding option.

29.Chinese Researchers Claim To Have Broken RSA With A Quantum Computer. Experts Aren't So Sure.

by Alexander Martin
https://therecord.media/chinese-researchers-claim-to-have-broken-rsa-with-a-quantum-computer-experts-arent-so-sure/

Researchers in China claim to have reached a breakthrough in quantum computing, figuring out how they can break the RSA public-key encryption system using a quantum computer of around the power that will soon be publicly available.

Breaking 2048-bit RSA — in other words finding a method to consistently and quickly discover the secret prime numbers underpinning the algorithm — would be extremely significant. Although the RSA algorithm itself has largely been replaced in consumer-facing protocols, such as Transport Layer Security, it is still widely used in older enterprise and operational technology software and in many code-signing certificates.

If a malicious adversary were able to generate these signing keys or decrypt the messages protected by RSA then that adversary would be able to snoop on internet traffic as well as potentially pass off malicious code as if it were a legitimate software update, potentially enabling them to seize control of third-party devices.

These issues are a key part of the threat that quantum computing poses to traditional cryptography. In a white paper published by the U.K.'s National Cyber Security Centre in November 2020, experts warned that because almost all of today's widely-used public-key cryptography systems depend for their security on the difficulty of factoring very large numbers, they would be easy to crack with a large-enough general purpose quantum computer.

The Chinese researchers' paper, titled "Factoring integers with sublinear resources on a superconducting quantum processor," features one of the first claims that this can now be practically achieved. They argue that they can break the 2048-bit algorithm using a 372-qubit quantum computer. There are some caveats, however. They only had access to a 10-qubit device to practice on and were unable to demonstrate their hypothesis on anything larger than 48-bits.

Many experts are questioning their findings. The paper itself has been shared through the preprint service arXiv without any meaningful peer-review, something which would generally be considered a necessary minimum standard to weigh the scientific value of a research paper.

A discussion about the paper on Google Groups challenges whether the paper claims that its method for factoring 2048-bit integers is actually any faster than classical methods. Both that discussion, and analysis by cryptography expert Bruce Schneier, warns that the researchers' algorithm relies on a controversial paper by the German mathematician Peter Schnorr which, while proving an ability to factorize numbers on the scale of the 10-qubit computer used by the researchers, "falls apart at larger sizes."

Schneier wrote that after the criticism of the paper's dependence on Schorr's algorithm was raised with him he was "much less worried that this technique will work now."

According to the arXiv publication, the authors are affiliated with some of China's most prestigious universities, including several State Key Laboratories which receive direct funding and support from Beijing. Security experts who have spoken to The Record said they expected that a scientific breakthrough with such a significant security impact would be classified by the Chinese authorities.

Historically there have been examples of such information leaking out against the wishes of the ministries in Beijing. Alibaba Cloud was reportedly sanctioned by the Ministry of Industry and Information Technology after a worker there was credited with disclosing the Log4J vulnerability to the Apache Software Foundation instead of to the Chinese government.

The Cyberspace Administration of China had introduced stricter rules a few months before, in July 2021, around disclosing vulnerabilities for companies operating within its borders. For its part, Microsoft last November accused state-backed hackers in China of abusing these vulnerability disclosure requirements in an effort to discover and develop their own zero-day exploits.

30.Quantum's Promise

by Andrew Singer
https://www.gfmag.com/magazine/january-2023/quantum-computing-promise

Early in October, US President Joe Biden traveled to Poughkeepsie, New York, and stood shoulder to shoulder with IBM executives as they announced that the company would be spending $20 billion on production of semiconductors and development of advanced technology like artificial intelligence (AI) and quantum computing (QC) research.

Both AI and QC will be critical for corporate effectiveness and national security in coming years. Linking AI and QC in the same news cycle was understandable too, given that QC represents to some degree the logical extension of AI.

AI is often used in automating tedious tasks. Many of its achievements, such as facial recognition, are simply the result of raw computing power. Quantum tech expands computing power exponentially. Some believe it will eventually help doctors identify cancers earlier, pharmaceutical companies bring drugs to market faster, extend the life of batteries and more.

It may not take decades before real-world solutions emerge, either. "If publicly available vendor road maps hold, it is entirely possible to have quantum-enabled AI use cases in five years," says Scott Buchholz, emerging technology research director and CTO for Government and Public Services at Deloitte Consulting.

Indeed, some believe corporate and government leaders should begin laying out quantum-computing strategies now, "especially in industries, such as pharmaceuticals, that may reap the early benefits of commercial quantum computing," says consulting firm McKinsey. While most activity is still in research or pilot phase, a few startups like Paris-based QC firm Pasqal are getting close to rollout. Pasqal already has a customer list that includes Johnson & Johnson, LG Electronics, Airbus, BMW, EDF, Thales, MBDA and Credit Agricole CIB.

Quantum computing is based on "qubits" (quantum bits), which are the smallest units of quantum information, analogous to the regular computer bit. Qubits, IBM explains, “harness quantum mechanical phenomena ... to solve problems that are fundamentally intractable for classical computers.”

The sheer power of QC is mind boggling. A 2017 article in Scientific American claimed that “in principle, a 300-qubit quantum computer could perform more calculations at once than there are atoms in the observable universe.” That statement is now oft-repeated industry lore. Pasqal’s processors have already reached 100 qubits—close to the 127 qubits of IBM’s ground-breaking Eagle—and Pasqal expects to bring a 1,000-qubit processor to market by the end of 2023. Meanwhile, companies like IBM, Microsoft, Google and Honeywell have been investing heavily to expand the technology. In November, IBM unveiled its 433-qubit quantum processor called “Osprey.”

“Quantum computing has the potential to ultimately be game changing in a number of ways,” says Charles Toups, vice president and general manager for Boeing Disruptive Computing and Networks. It could enable the aerospace giant to model complex materials more accurately and also “faster than we are able to complete small-scale, lower fidelity models today,” he says. Boeing sees promise, too, in using QC to model detailed chemical reactions “that will help us devise longer lasting protections for corrosion and ultraviolet exposure.”

The first areas likely to receive a QC boost are optimization, machine learning (ML—an essential component of AI, the terms are often used interchangeably) and predictive modeling, where finding solutions is “fiendishly difficult” but can be easier with quantum computers, given their “ability to handle data that has high degrees of ‘optionality,’” or dimensionality, Buchholz adds

“This is the quantum decade,” says Konstantinos Karagiannis, director, Quantum Computing Services at Silicon Valley consultant Protiviti. “The uses aren’t as far away as most people think.”

One type of proto-quantum computer already in use is the “quantum annealer.” Annealers work hand in hand with classical computers to solve optimization problems like routing trucks or assembling factories. But this is just a taste of things to come, especially when gate-based “universal” QC machines pioneered by IBM, IonQ and others reach the market. “Those are the ones that have the potential one day to crack encryption and do some of those bad things,” Karagiannis adds, “but also to change the world, because quantum machine learning will run better on them.”

Protiviti is now employing a gate-based quantum computer for fraud detection, a typical ML classification use case. “There are only a handful of machines on the cloud that are powerful enough to do it. You have to wait for your turn to run it,” says Karagiannis.

Possible Eco Benefits

The field appears to be well funded. Venture capital firms alone invested more than $1 billion into the sector in 2021, according to Deloitte, which says the industries likely to gain first from the technology include pharmaceuticals, chemicals (catalysts, more eco-friendly feedstocks), automotive (optimized factory-robot motions) and finance (investment portfolio optimization).

QC offers potential ecological benefits too: Quantum computers using “quality” qubits (still not commonly available) could make high-level computing dramatically more energy efficient, according to Interesting Engineering. “There are tasks for which the quantum computer could spend one hundred times less energy than the best current supercomputers.”

Quantum-enabled AI also has a national security aspect. Some believe China has gotten the jump on the US and other Western nations in the AI race, and Bloomberg reported in mid-October that the US may soon place export controls on AI and QC technologies. Others worry that QC could one day break the algorithm used for the public-key encryption that allows secure transmission of email and much of modern communications.

Quantum-Enabled AI

While use cases involving universal QC are still rare, more companies announced AI/QC initiatives in the past year. LG Electronics is exploring QC for big data, IoT, AI, robotics and other applications that, LG notes, all require processing a large amount of data. Meanwhile, HSBC is also looking at QC for investment portfolio optimization, risk mitigation and fraud detection, which typically use ML algorithms to process large amounts of data.

This is the first technology that is truly exponential, says Karagiannis. Many people today are familiar with Moore's Law, which roughly states that computer power doubles every two years. But Moore's Law pales beside QC's projected growth curve, where a system's power doubles every time a single qubit is added. "[If] someone has a 100-qubit machine and then someone else has a 200-qubit machine, that's many, many orders of magnitude more powerful, not just double," Karagiannis explains.

Building on the success of its 127-qubit Eagle, IBM in 2023 will deliver the Condor, "the world's first universal quantum processor with over 1,000 qubits," according to the company,   and a 4,000+ qubit processor by 2025.

Not surprisingly, obstacles remain before these science fiction-like capabilities can be realized. A quantum computer is not just a scaled-up version of today's supercomputers. "It's something very different," says Deloitte's Buchholz. "We are attempting to constrain individual atoms and particles to behave in a regimented fashion, which is not their natural state." They need to be interconnected, contained and constrained, something "unthinkable" a decade ago.

"Some approaches to quantum machine learning introduce completely novel ways to do machine learning that do not have a classical analogue," says Vedran Dunjko, associate professor at the Netherlands' Leiden University. But many of these "novel" uses are many years away—and may never be realized. In terms of first applications, Dunjko anticipates use cases close to quantum technologies, as in the development of exotic materials.

German conglomerate Bosch also believes that quantum computers may soon offer "a significant advantage over conventional computers in discovering and designing new materials" for products like fuel cells, batteries, electric engines or advanced sensors. "Classical computers are not able to calculate the properties of these materials with sufficient accuracy," the company commented recently in announcing its new partnership with IBM to develop quantum algorithms for industrial applications.

Aerospace firms are watching developments closely too. "Harnessing quantum technologies for the aerospace industry is one of the great challenges we face in the coming years," commented Greg Hyslop, Boeing's chief engineer and executive vice president of engineering, testing and technology, in discussing Boeing's $5 million gift for faculty research in quantum science.

"The emergence of some small-scale prototypes of QC has already propelled the development of post-quantum cryptography," says Takaya Miyano, a professor of mechanical engineering at Japan's Ritsumeikan University. He expects to see the first practical uses of QC for cryptography and the military as well as pharmaceuticals.

The US-China Rivalry

"AI and quantum computing are among the most important technologies for the next decade and beyond," Jonathan Panikoff, senior fellow at the Atlantic Council's Geoeconomics Center and director of its Scowcroft Middle East Security Initiative, tells Global Finance. AI and QC are also "very likely to underlie portions of US-China competition for the coming decades as well."

Admittedly, it may take time before this all plays out. Devices like China's powerful 66-qubit Zuchongzhi processor "are not capable of universal quantum computation and cannot play a role in such geopolitical struggles," Marek Narozniak, a physicist and member of a quantum research group at New York University, tells Global Finance.

Still, in one study, Chinese researchers found that Zuchongzhi was able to complete a sampling task in 1.2 hours that they estimated would have required a 2019 classical supercomputer 8.2 years to complete. But even study co-author Chao-Yang Lu acknowledged that the sample task completed had no practical value, adding that "the computational problems that can truly benefit from quantum computing are still quite limited," as quoted in Physics World.

Governments are paying attention too. In May, a US National Security Memorandum flagged the potential "risks of quantum computers to the nation's cyber, economic and national security," and directed US agencies to begin a "multiyear process of migrating vulnerable computer systems to quantum-resistant cryptography."

That White House memo "accurately captured the challenges quantum computing could pose to Western interests across the economy, finance, infrastructure and national security sectors," Panikoff comments, while adding that "quantum computing and its uses, including for nefarious purposes, is still in its infancy and developing."

Much Fanfare, Little Utility

What about critics like Oxford University physicist Nikita Gourianov, who recently wrote in the Financial Times that "the quantum computing industry has yet to demonstrate any practical utility, despite the fanfare"?

"There have not yet been any clear demonstrations of practical utility," answers Boeing's Toups. The critics have a point. "However, based on our investigations, we see great promise to eventually be able to use quantum computers to make practical improvements that will dramatically improve our products and services."

"Those quotes always baffle me," comments Karagiannis "There are about 140 companies that are currently using D-Wave [quantum annealers] in real business applications daily."

In a test run, Volkswagen used live access to a D-Wave quantum processor to optimize the painting process in one of its factories.

"For example," a case report by D-Wave Systems explains, "if a small subset of minivans was slated to be painted black rather than white, the algorithm would specifically assign those paint jobs to minivans falling within stretches of the production run where other vehicles are already being painted black."

Volkswagen later reported, "We managed to reduce the color switches in the entire sequence significantly."

Still, as noted, D-Wave machines, which debuted in 2011, are basically analog computers, "meaning they only tackle one specific problem," Samuel Mugel, CTO at Multiverse Computing, a quantum software development company, tells Global Finance. "They are not equivalent to universal quantum computers, which can tackle any problem." And regarding the latter, the technology isn't ready for mainstream industrial use, as even Karagiannis acknowledges.

“Right now, we’re in the ‘noisy’ intermediate-scale quantum era,” Karagiannis says. “The qubits interfere with each other. The support circuitry interferes. It’s really hard … It’s hard to get these machines to stay in a behaving state.”

But the buzz is rising. “It’s almost inevitable that there will be under- and overselling as we transition from research to engineering to application,” adds Deloitte’s Buchholz.

“It is easy to be a naysayer and negative these days,” says Dunjko. He prefers to focus on how far QC has evolved since he began working in this area in 2010. “Even if technology continues just linearly, we will have tremendous devices.”

Technology does not advance linearly, of course. Progress is more a stop-and-start affair. “Creative new ideas cause disruptive jumps,” Dunjko adds, so when projecting the long-term impact of quantum-enabled AI, some intellectual humility may be in order.

“In the same way that it was impossible to understand the impact of digitalization in the 1960s or the internet in the 1990s, we have only the barest inklings today of what might be possible,” Buchholz says.