Crypto News

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

December 01, 2022

TABLES OF CONTENTS

Editorial

Season's greetings readers! Let's jump right in with article 1 in this month's newsletter which talks about "Why cryptographers are worried about a post-quantum world". In a nutshell, our secrets are no longer going to be a secret. More specifically, the algorithms that allow for secure browsing, online shopping, bill payments, etc., are all vulnerable to quantum computers. So, should you be worried? The author of the article states that the answer is "yes". Though that may sound concerning and potentially cause you to push the panic button in your mind, know that hope is not lost. One of the solutions being explored is a theoretical quantum internet. The quantum internet would work based on quantum computing theory including quantum entanglement and quantum steering. If you'd like to learn more about the theoretical quantum internet, scroll down to article 25 to gather more insight.

Then, check article 6 to see if the industry you work in is one of the nine at risk when quantum computers show a quantum advantage. Do you happen to work in banking? What about life sciences or consumer electronics? Depending on which field you work in, you are encouraged to take action immediately, in the short term, or long term to be ready for a post-quantum world. Regardless of the timeline, one thing for sure is that action must be taken and the sooner you are able, the better for your organization. Now you're going to want to read article 20 to learn about how the "quantum computing arms race" between the United States of America, China, and Europe is getting heated. Their competition is the reason for the current growth of the quantum ecosystem. It seems that the healthy (but likely somewhat contentious) competition between the nations is resulting in promoting advancements in quantum computing. Who do you think will win this arms race?

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.Why Cryptographers Are Worried About A Post-Quantum World

by Joppe W. Bos

https://www.embedded.com/why-cryptographers-are-worried-about-a-post-quantum-world/

Device connected to the Wi-Fi router? Check. Bills paid online? Check. And, while doing those things, did you stop to consider how secure those actions were? Unlikely. Since the wild-west feeling of the internet's introduction back in the 1990s, we've left security to the experts. And they've done an excellent job. While passwords are stolen and access is hacked, the algorithms that implement security, such as AES (advanced encryption standard) and ECC (elliptic-curve cryptography), remain unbroken.

Today's cryptography relies on four things. The first is math problems, which are easy to solve if you know the secret key but almost impossible if you don't. Actually, this point needs clarification – almost impossible using today's computing capability. Secondly, the algorithm must not have weaknesses. The longest attack is a brute force approach, trying all possible keys until the correct one is found. Researchers using cryptanalysis (the science of breaking codes) sometimes find shortcuts that reduce the number of keys they need to try, making key discovery simpler.

The third aspect is implementation. It's no good selecting a secure algorithm if executing the implementation somehow leaks the secret key used. The final element is human – we need to keep our secrets, well, secret. Because today's systems are so challenging to crack, hackers prefer to use social engineering to get us to give up passwords and circumvent two-factor authentication systems. We need to remain aware of such schemes and how to avoid being drawn in.

And then quantum computing appeared…

Until recently, all was well with cryptography. As computing power has grown, AES and ECC have used increasingly longer keys, ensuring that brute force attacks require as long now as they did with shorter keys a decade before. But unfortunately, computer performance is no longer growing at a steady pace. Instead, it is making a quantum leap.

Quantum computers change the status quo when it comes to performing calculations. Unlike digital processors with their ones and zeros, quantum computers harness the power of quantum mechanics using quantum bits (qubits). These machines will have the potential to deliver tremendous benefits for humanity, such as simulating complex biological systems that lead us to improved medical therapies. But they also make some of today's complex math problems look like child's play: unfortunately, some of these math problems form the foundation for our current cryptographic standards.

Today, quantum computers are exceptionally expensive and complex to operate, and the largest has less than 200 qubits. However, the speed with which the number of qubits increases in these machines is worrying. Knowing that only around 4,000 stable qubits are required to break RSA-768 encryption (and more for the larger versions of RSA which are used in the field) it really is only a matter of time before Internet security, as we know it, is broken.

Cryptographers are ready

The risks of quantum computers to cryptography have been apparent for some time. This led NIST, the

National Institute of Standards and Technology, to launch a competition in 2016 to find new, quantum-resistant algorithms. This year, in 2022, the first four algorithms were announced.

The challenge for NIST was finding algorithms that were both quantum-secure and suited to today's Internet applications. While computers and smartphones have ample processing power and memory, billions of small, microcontroller-powered internet of things (IoT) devices are being added every day. These devices have limited computing performance, kilobytes of memory, and must draw so little energy that their batteries last for years.

CRYSTALS-Kyber has been selected for key exchange, an algorithm NXP helped develop. Noted for its comparatively small key size (although much larger than what we're used to) and speed of operation, it relies on the learning-with-errors (LWE) problem over module lattices.

Digital signatures have received three possible alternatives. CRYSTALS-Dilithium and FALCON also make use of lattice-based cryptography and are pretty efficient. To provide mathematical diversity, SPHINCS+ has also been selected. Slower, by comparison, this algorithm is a hash-based signature scheme.

Moving to post-quantum cryptography

While the algorithms have been selected, there is still some work to do before we can start using them. One aspect is implementation – how will key exchange occur, and what will security certificates look like? Another is hardware support. Work has already been undertaken to test the software, with benchmarks available for the workhorse of embedded systems, the Arm Cortex-M4. However, there is still much to do.

Many processors acquired additional instructions to optimize the execution of AES, and dedicated security chips that support ECC are available from various semiconductor vendors. We should expect quantum-secure hardware to emerge in the next couple of years in the form of dedicated instructions, hardware acceleration IP, and dedicated security chips.

Researchers have undertaken much work around security implementation over the years. Power and RF analysis, coupled with decapping and probing, have uncovered weaknesses in security chips. The semiconductor industry has responded, ensuring that devices are less "leaky" by implementing suitable countermeasures. These are currently considered adequate, even as we move into a post-quantum era but will have an additional impact on the size and practical performance.

What can I do today?

Today, there is little that can be done practically to move to quantum cryptography. However, there are ways to prepare. Perhaps the most important is to ensure that good IT security practices continue to be promoted. There is a significant risk that bad actors will go on a data harvesting spree, collecting encrypted data and communications, knowing they will be able to crack security keys in the coming years. And this won't require possessing a quantum computer – it's expected that these will be offered at hourly rates as a cloud service.

Security audits are another planning task, understanding what encryption is used and where, and what data and systems will require updating. For those developing new IoT solutions or maintaining existing ones, it is time to start the quantum conversation with hardware, software, and service suppliers to understand their security upgrade plans. Finally, talk to semiconductor vendors to learn what they are planning and how it will change the implementation of security in your products.

2.Solving The Quantum Threat With Post-Quantum Cryptography On EFPGAs

by Flex Logix

https://semiengineering.com/solving-the-quantum-threat-with-post-quantum-cryptography-on-efpgas/

Advances in quantum computing technology threaten the security of current cryptosystems. Asymmetric cryptography algorithms that are used by modern security protocols for key exchange and digital signatures rely on the complexity of certain mathematical problems. Currently, the main problems used for asymmetric cryptography are integer factorization of RSA and elliptic curve discrete logarithm of the elliptic curve cryptography (ECC). Shor's algorithm is a quantum algorithm that can solve these problems if a large enough quantum computer is built. As a consequence, this would break the related cryptosystems and the basis of current computer and communication security. Although quantum computers of cryptographic significance do not exist today, many systems designed now will be in use for decades. It is also possible to record data today and break it in the future when powerful quantum computers will be available.

The international security community woke up to this quantum threat several years ago and developed ways to mitigate it. Post-quantum cryptography (PQC) are algorithms that run on traditional computers but are based on mathematical problems that cannot be solved efficiently with Shor's algorithm, or by any other known quantum computing algorithm. Unique solutions will be required to solve this complex problem and many people are researching it. In 2016, the National Institute of Standards and Technology (NIST) of the United States initiated a competition to find solutions to standardize PQC algorithms. After three rounds, the competition concluded in July 2022 with the publication of four winning algorithms that will be standardized: CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+. Kyber is a so-called Key Encapsulation Mechanism (KEM) that is used for key exchange and the rest are digital signature algorithms. NIST continues the competition with a fourth round to find even further advanced PQC algorithms for a more robust standard in the future. Although the algorithms to be standardized are now known, they may still be tweaked before even the draft standards are written. The final standards are expected to be published in a couple of years and may still change from what is known today.

System designers need to start shifting to PQC immediately, as many organizations and formal requirements mandate security systems to support PQC in the near future. The recent announcement by the National Security Agency (NSA) mandates certain US national systems to support PQC in 2025. These requirements, combined with the still changing PQC landscape, set very high needs for crypto agility: the ability to update and change cryptographic algorithms in deployed systems. There are some solutions being proposed.

3.Defeating A Cryptoprocessor With Laser Beams

by Arya Voronova

https://hackaday.com/2022/11/26/defeating-a-cryptoprocessor-with-laser-beams/

Cryptographic coprocessors are nice, for the most part. These are small chips you connect over I2C or One-Wire, with a whole bunch of cryptographic features implemented. They can hash data, securely store an encryption key and do internal encryption/decryption with it, sign data or validate signatures, and generate decent random numbers – all things that you might not want to do in firmware on your MCU, with the range of attacks you'd have to defend it against. Theoretically, this is great, but that moves the attack to the cryptographic coprocessor.

In this BlackHat presentation (slides), [Olivier Heriveaux] talks about how his team was tasked with investigating the security of the Coldcard cryptocurrency wallet. This wallet stores your private keys inside of an ATECC608A chip, in a secure area only unlocked once you enter your PIN. The team had already encountered the ATECC608A's predecessor, the ATECC508A, in a different scenario, and that one gave up its secrets eventually. This time, could they break into the vault and leave with a bag full of Bitcoins?

Lacking a vault door to drill, they used a powerful laser, delidding the IC and pulsing different areas of it with the beam. How do you know when exactly to pulse? For that, they took power consumption traces of the chip, which, given enough tries and some signal averaging, let them make educated guesses on how the chip's firmware went through the unlock command processing stages. We won't spoil the video for you, but if you're interested in power analysis and laser glitching, it's well worth 30 minutes of your time.

You might think it's good that we have these chips to work with – however, they're not that hobbyist-friendly, as proper documentation is scarce for security-through-obscurity reasons. Another downside is that, inevitably, we'll encounter them being used to thwart repair and reverse-engineering. However, if you wanted to explore what a cryptographic coprocessor brings you, you can get an ESP32 module with the ATECC608A inside, we've seen this chip put into an IoT-enabled wearable ECG project, and even a Nokia-shell LoRa mesh phone!

4.Space Tracking Company Adds Quantum-Safe Encryption

by Ryan Morrison

https://techmonitor.ai/hardware/post-quantum-encryption-space

A company that uses satellites to track ship movements has become the first in the world to offer post-quantum encryption end-to-end from the satellite to the cloud. French satellite company Unseenlabs worked with quantum encryption developer Secure-IC on the new protocols.

Unseenlabs has a fleet of satellites in low Earth orbit designed to track any vessel anywhere on the ocean at any time. Companies pay a subscription for access to this data, giving them the ability to locate and monitor vessels and keep them safe. It can also be used in the fight against pollution, illegal traffic, piracy and other negative impacts on the ocean and climate.

Some of the data being sent from space to the ground can be commercially sensitive and is already protected using the best current end-to-end encryption authentication protocols, but that won't protect the information when quantum computers reach maturity.

At some point within the next ten to 15 years experts predict quantum computers will become powerful and error-free enough to crack even the best encryption techniques within a day or less – something classical computers would need tens of thousands of years to achieve.

To combat this risk, companies, governments and organisations are working on post-quantum encryption algorithms using maths problems that even a quantum computer couldn't easily solve and Unseenlabs is the first satellite fleet operator to implement this throughout its network.

The US National Institute for Standards and Technology (NIST) has been holding a competition since 2016 to source new standards for encryption algorithms that, in theory, should be able to withstand the codebreaking abilities of mature quantum computers. So far, four have been put forward as standards, and have yet to be cracked.

It isn't clear exactly which algorithms are being deployed by Unseenlabs on its fleet of seven satellites but it is being launched as part of a security integration platform similar to those used in Internet of Things devices and fleets of equipment managed by large companies. It will be available on the most recent pair of satellites launched by the company – bro-6 and bro-7 – that launched earlier this year.

Making post-quantum encryption future-proof

The new project, dubbed bro-pqc, will see the platform deployed to the existing seven spacecraft as well as all future satellites, including the integration of current and post-quantum cryptography solutions. The company says this allows it to future-proof its authentication.

“It is augmented with the ability to notarise information arising from the satellites and secure data using post-quantum cryptography,” an Unseenlabs spokesperson explained, adding that the service is powered by Securyzr™ technology, a cybersecurity lifecycle management platform built by Secure-IC for connected objects. It allows companies to deploy and manage fleets from the cloud – which is vital when your fleet is hundreds of miles above the Earth in the vacuum of space.

“With the ‘bro-pqc’ project, we aim to leverage post-quantum cryptography to provide state-of-the-art and future-proof authenticity of the data which is measured from LEO and subsequently downloaded to Earth,” says Jonathan Galic, Unseenlabs CTO and co-founder.

“Secure-IC offerings deliver the flexibility, performance and capability we were looking for, which are needed in order to deliver tangible, near real-time data and secure data to our clients,” Galic adds.

The Securyzr™ technology will allow the company to deploy the post-quantum solutions after launch, as well as make updates as new, more secure algorithms are developed. This is vital as post-quantum cryptography standards are still in development with many not tested or finalised.

“Our solutions are currently embedded into hundreds of millions of electronic chips for smartphones, computers, automobiles, smart meters, cloud servers and more,” says Sylvain Guilley, co-founder of Secure-IC and company CTO.

“The announcement of this partnership with Unseenlabs reaffirms Secure-IC's leading position in the embedded cybersecurity landscape and innovation in cutting-edge technologies.”

The company has been developing both hardware and software-based post-quantum solutions and adapting it for ‘internal security’ running on device firmware that can then be deployed and updated as the algorithms improve.

5.Mathematical Theorem Used To Crack Us

Government Encryption Algorithm

by Catarina Chagas

https://phys.org/news/2022-11-mathematical-theorem-encryption-algorithm.html

In the digital era and moving towards quantum computing, protecting data against hack attacks is one of our biggest challenges—and one that experts, governments, and industries worldwide work hard to address. While this is an effort to build a more connected and safe future, it can certainly learn from the past.

In July, the US National Institute of Standards and Technology (NIST) selected four encryption algorithms and posed some challenge problems to test their security, offering a $50,000 reward for whomever managed to break them. It happened in less than an hour: one of the promising algorithm candidates, named SIKE, was hacked with a single personal computer. The attack did not rely on a powerful machine, but on powerful mathematics based on a theorem developed by a Queen's professor decades ago.

Ernst Kani has been researching and teaching since the late 1970s—first at the University of Heidelberg, in Germany, and then at Queen's, where he joined the Department of Mathematics and Statistics in 1986. His main research focus is arithmetic geometry, an area of mathematics that uses the techniques of algebraic geometry to solve problems in number theory.

The problems Dr. Kani works to solve stretch back to ancient times. His specific field of research was pioneered by Diophantus of Alexandria around 1,800 years ago and is a set of problems known as Diophantine questions. One of the most famous questions in the field is Fermat's Last Theorem, posed by Pierre Fermat in 1637 and which took the math community 350 years to prove—an accomplishment by Princeton professor Andrew Wiles in 1994. Wiles received many prizes and honors for this work, including an honorary doctorate from Queen's in 1997.

Neither Diophantus nor Fermat dreamt of quantum computers, but Dr. Kani's work on Diophantine questions resurfaced during the NIST round of tests. The successful hackers—Wouter Castryck and Thomas Decru, both researchers at the Katholieke Universiteit Leuven, in Belgium—based their work on the "glue and split" theorem developed by the Queen's mathematician in 1997.

As a matter of fact, Dr. Kani was not concerned about cryptographic algorithms when he developed the theorem. That work kicked-off in the 1980s, in collaboration with another German mathematician, Gerhard Frey—whose work was crucial in solving Fermat's last theorem. Drs. Kani and Frey wanted to advance research on elliptic curves, a particular kind of equation that would later be used for cryptographic purposes.

Both researchers' goals at that time were purely theoretical. They were interested in manipulating mathematical objects to learn more about their own properties. "Doing pure mathematics is an end by itself, so we don't think of real-world applications," Dr. Kani explains. "But, later, many of those studies are useful for different purposes. When Fermat proposed his theorem hundreds of years ago, his intent was to be able to factor certain large numbers. The application to cryptography came only much later in 1978. Basically, all the methods we use today for data encryption are based on mathematics.”

Doughnuts and curves

Mathematicians often refer to mathematics as a beautiful thing. For those who don't work in the field, it might be challenging to see this beauty, or even to have a high-level understanding of what these research projects are all about—it requires some imagination.

Imagine an object shaped like a doughnut, with a hole in the middle: that's a visual model of an elliptic curve, also known as a genus one curve. Drs. Kani and Frey wanted to combine two genus one curves to form a new object—a genus two curve, something we can imagine like two doughnuts stuck solidly together side by side. They aimed to use some properties of the constructed genus two curve to deduce certain properties of the two original genus one curves, which were "glued" together.

In his 1997 paper, Dr. Kani generalized the original construction by gluing together an arbitrary pair of elliptic curves. But in that case the construction sometimes fails—it might construct an object in which the two doughnuts only touch each other in a single point. The paper analyzes the precise conditions for when this happens (i.e., when the construction fails or "splits"). Castryck and Decru used this characterization of the failure in their method of attacking the proposed encryption scheme SIKE.

"Our problem had nothing to do with cryptography, which is why I was surprised when I heard of the algorithm attack. It was quite ingenious, what they did there!" says Dr. Kani. "One of the co-authors of the SIKE algorithm expressed surprise in the fact that genus two curves could be used to gain information about elliptic curves. But this was precisely our original strategy in the 1980's and 1990's (and afterwards)."

Although cryptographers and computing engineers are not always well-versed in all the high-powered techniques of mathematics, many different skills and forms of knowledge can be combined to advance the way we store and transmit data.

"Cryptography uses a lot of sophisticated mathematics, especially arithmetic geometry. Computing experts and math experts have to work together to advance this field," says Dr. Kani, who continues to teach undergraduate and graduate courses and to work in arithmetic geometry—particularly on problems involving genus two curves and elliptic curves.

6.Post-Quantum Cryptography: Nine Industries At Risk From "Y2Q"

by John Kilhefner

https://www.spiceworks.com/it-security/security-general/guest-article/post-quantum-cryptography-nine-industries-at-risk-from-y2q/

Y2Q is short for "year 2 quantum" and refers to the year when quantum computers are expected to become powerful enough to break today's encryption standards. This poses a serious threat to the security of our networks and data, as quantum computers will be able to decrypt transmissions that are currently considered safe. John Kilhefner, security researcher at Vicarius, takes a closer look at nine industries most at risk from Y2Q and why.

To keep our information safe, we have come to depend on algorithms that rely on.

But because quantum computers can solve the factoring problem much faster than traditional computers, they pose a serious threat to the security of today's algorithmic standards – and by extension, the security of our networks.

One such standard in use today is, named for the MIT scientists who invented it (Rivest, Shamir, and Adleman). RSA came about in 1977 as an asymmetric algorithm using a public key for encryption. This is called public key cryptography, and it's the product of multiplying two prime numbers. Only the public key creators can generate the necessary private keys to decrypt the transmission. Such integer factorization is the basis for many of the most popular cryptographic algorithms today, including RSA and Diffie-Hellman.

Quantum systems, when available, will decrypt today's asymmetric security protocols, which are widely used to secure messages through public channels. And while symmetric encryption protocols are considered safe from the quantum threat, it's not practical to always use this method. Because in symmetric encryption, the sender and receiver both exchange encryption and decryption keys before any information trades hands, making it impractical when speed is required. So even symmetric encryption must be addressed for efficiency before "Y2Q" (year to quantum) arrives.

Of course, the best way to prepare for Y2Q is to stay ahead of the game by keeping up with advancements in quantum computing. This means investing in research and development so that we can create quantum-safe algorithms before they're needed. And it also means developing a better understanding of how quantum computers work so that we can anticipate their every move.

But regardless of what the future holds, one thing is certain: we must be prepared for the quantum threat. Because if we're not, Y2Q could be the end of encryption as we know it.

Once large-scale quantum computers are built, they will be able to that we currently use to protect our data. This includes popular protocols like TLS/SSL (used to secure HTTPS connections), SSH (used to secure remote access and file transfers), and IPsec (used to secure VPNs).

And while we have no way of knowing precisely the moment when the first fully error-corrected quantum computer will come online, we do know that certain industries are more at risk today than others. And these industries should now take steps to ensure their network security is ready for the age of quantum supremacy.

But the threat isn't equally distributed. So let's break down to the quantum threat at various points along the timeline:

Industries Most at Risk Now

- Insurance
- Public Sector
- Banking

Why: These organizations have data with long shelf lives and systems with extended cycles of development. This means bad actors could harness their data now and wait for quantum computing to come online to break their encryption.

At Risk Between 2025-2030

- Life Sciences
- Advanced industries
- Global energy and materials

Why: These organizations possess data and systems also have long shelf lives and therefore are at risk of being targeted after 2025 until quantum computing comes online.

At Risk After 2030

- Telecom, media and technology
- Consumer electronics
- Travel and logistics

Why: These organizations have shorter-duration data and, therefore, may not need to act immediately. However, they still need to act before quantum becomes truly capable.

As mentioned earlier, traditional cryptographic methods are vulnerable to attack by quantum computers. This means that if quantum computers become powerful enough, they could be used to break current encryption methods and access sensitive information.

So what can be done to prevent the “Y2Q” threat? The answer lies in post-quantum cryptography, or “PQC,” which we discussed in depth in the first part of this story.

To recap, PQC is a type of cryptography that is designed to be resistant to quantum computers. There are a variety of different PQC algorithms that have been developed, each with its own strengths and weaknesses.

Ways for Security Researchers to Mitigate the Threat

Post-quantum cryptography is an important step in protecting information from quantum computer attacks. And if you’re a security researcher, it’s crucial that you start preparing for the migration to PQC now. By familiarizing yourself with the basics of PQC and experimenting with different algorithms, you can ensure that you are prepared for the future of quantum computing.

Fortunately, there are steps you can take today to protect your network security against quantum computing attacks.

- **First**, make sure you have a good understanding of what PQC is and how it works. This will help you make informed decisions about which PQC algorithms to use and how to implement them properly.

- **Second**, start experimenting with PQC algorithms now. Several different algorithms are available, so it’s important to find one that works well for your needs. For example, some PQC algorithms are faster than others, while some are more secure. But perhaps the best way to protect data against quantum computers is to use a hybrid encryption approach, which combines the strengths of both symmetric and asymmetric encryption. This way, even if one of the methods becomes compromised, the other will still keep our data safe.

- **Third**, look into (MPC). MPC allows two or more parties to compute a function while keeping their inputs secret. This means that even if an attacker compromises one party, the attacker will not be able to learn anything about the other party’s input. As a result, MPC has been shown to be resistant to both classical and quantum attacks.

- **Fourth**, you can protect your data through (QKD). QKD takes advantage of the laws of physics to distribute cryptographic keys securely between two parties. Because an attacker cannot read these keys without introducing errors into them, QKD provides resistance against both classical and quantum hacking attempts.

- **Lastly**, keep up with the latest developments in PQC. While post-quantum cryptography is still in its early stages, a few major approaches are being researched:

    - **Lattice-based cryptography**: These schemes are based on the hardness of certain mathematical problems over high-dimensional lattices. The most popular lattice-based scheme right now is called Ring-LWE.

- **Code-based cryptography:** These schemes are based on the hardness of decoding certain error-correcting codes. The most popular code-based scheme right now is called McEliece.
- **Hash-based cryptography:** These schemes are based on the one-wayness of cryptographic hash functions. The most popular hash-based scheme right now is called Sphincs+.

In addition to these three major approaches, there are also a few miscellaneous schemes that don't really fit into any particular category, like **quantum key distribution** and **post-quantum zero-knowledge (PQZK)**.

A Cryptography Scheme that Works for You

So which post-quantum cryptography scheme is the best? Well, that's a bit of a loaded question since there is no "best" post-quantum cryptography scheme. Each scheme has its own advantages and disadvantages, and it really depends on your particular needs as to which one is the best for you.

For example, if you need a post-quantum digital signature scheme, then you might want to look at hash-based schemes like Sphincs+. On the other hand, if you need a post-quantum key exchange protocol, then you might want to look at code-based schemes like McEliece or lattice-based schemes like Ring-LWE.

The post-quantum cryptography (PQC) initiative is already underway to standardize new protocols that quantum computers can't compromise. It's important to remember, however, that even with PQC in place, quantum computing is still in its infancy, and there is a chance that it may eventually become powerful enough to break PQC algorithms. But by staying informed, we can ensure that our data is as safe as possible from the "Y2Q" threat.

7.With Crypto In Retreat, Central Banks Take A Quantum Leap To Cryptography

by Andy Mukherjee

https://www.business-standard.com/article/markets/with-crypto-in-retreat-central-banks-take-a-quantum-leap-to-cryptography-122112100095_1.html

In the chaos surrounding the collapse of Sam Bankman-Fried's empire, it's easy to lose sight of what has died in this year's crypto carnage and what lives on. The biggest casualty is "anarcho-capitalism," championed by engineer Timothy May in the 1990s as cyberspace interactions unconstrained by external regulation, taxation or interference — in short, an absence of government.

That libertarian zeal, coded in the DNA of Bitcoin and every other virtual token, won't survive the recent turmoil in the blockchain world. If investors must turn to courts to recover their FTX losses, they'll want intermediaries and protocols to be supervised and made safe to use. Risky shadow banking in the garb of letting people swap their fiat currency for digital assets is coming to an end.

What will thrive even after this year's meltdown, however, is cryptographic money.

The idea of security without identification had come from privacy pioneer David Chaum, who invented the so-called blind signature in 1982. A decade later, eCash, the world's first digital currency, would deploy the technique. The anarcho-capitalists liked cryptography for its promise "to make Big Brother obsolete" — half the title of a celebrated 1985 paper by Chaum. Yet, in 2022, the biggest potential customer of these tools is none other than central banks, entities at the apex of states' financial power. What looked like a weapon of anarchy to May's cypherpunk movement has been repurposed as a technology for preserving and updating the existing monetary order.

Chaum is himself collaborating with a Swiss National Bank official on a blueprint for eCash 2.0, pitching it as "provably protected against counterfeiting even by a quantum computer" and "an ideal candidate for central bank digital currency." If the protocol proves roadworthy, the curmudgeonly public sector will reinvent itself as the the 21st-century's leading provider of a token more private than cash and yet more unfriendly to criminals. The private-sector crypto industry will have to play second fiddle to this better money.

The Bank for International Settlements is running a project around the ideas proposed by Chaum and his co-author, Thomas Moser, an alternate member on the SNB governing board. Project Tourbillon will explore the best possible mix of resiliency, scalability and privacy in a prototype central bank digital currency.

As shown by Ethereum co-founder Vitalik Buterin, blockchain-based payment systems face a trilemma. Everyone wants more secure networks. But the more complex the cryptography, the slower the system's scalability, or capacity to handle a large number of transactions. To make things go fast when there is both a technical and an economic limit on how many consensus-based decisions can be made and incentivized per second, you may need to skimp on decentralization, leaving the network vulnerable to attacks by bad actors or diluting the privacy guarantees.

Chaum and Moser have a solution. To boost speed to the levels of Visa Inc. and PayPal Holdings Inc., they're proposing a network that isn't based on distributed ledger technology, though it's possible to connect eCash 2.0 to a public blockchain. To enhance privacy, they're making the currency anonymous. But all senders of money will have an irrevocable right to undo the anonymity of any value withdrawn from their accounts: Malware won't be able to hide behind small users to aggregate and move large sums. (Even banks find it a tough problem to solve. Recall the scandal around Commonwealth Bank of Australia's cash machines, used by mules of a drug syndicate to launder millions of dollars.)

Finally, to boost security, the researchers are promising to deploy what the U.S. Department of Commerce's National Institute of Standards and Technology has found to be the strongest-known type of quantum-resistant cryptography. No wonder the staid world of central banking is excited about the prototype that will emerge from Project Tourbillon. It could well be the digital money everyone's waiting for — one that doesn't scare people away with the threat of 24x7 surveillance. "If you choose to use government-issued money, the government should not be able to see how you spend it," Chaum told CoinDesk. Users, however, should be able to protect themselves from being scammed.

If Tourbillon is a success, it could have both wholesale and retail applications. For end-consumers, the experience of transacting in central bank digital currency will be just like withdrawing physical cash from their bank accounts — except their phones will act as ATMs. Where there's no internet, payments will be secured with the help of an additional card. On the back end, freedom from the speed limits of distributed ledger technology could enable banks to use eCash 2.0 issued by their monetary authorities to move money across borders in seconds, leading to huge cost savings for small firms and consumers globally.

It was Mark Zuckerberg's now-abandoned idea of Libra, a new global currency to meet the "daily financial needs of billions of people," that shook authorities: Their monopoly on money was under siege. But now that they have joined the fight, central banks are in no mood to leave any corner of finance fully in the sway of the private sector. The monetary authorities of Switzerland, Singapore and France are exploring ways to automate currency exchange via smart contracts. These self-executing computer codes are the bedrock of decentralized finance, founded on the utopian premise of freedom from both governments and large custodial organizations. After this year's debacles in the world of digital assets, it's clear that the state is here to stay — not by repressing consumer choice but by using cryptography to offer a superior alternative.

8.Securing Tomorrow Today: Why Google Now Protects Its Internal Communications From Quantum Threats

by ISE Crypto PQC working group

https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms/?utm_source=linkedin&utm_medium=unpaidsoc&utm_campaign=fy22q4-googlecloud-blog-security-in_feed-no-brand-global&utm_content=cryptography-blog&utm_term=-

When you visit a website and the URL starts with HTTPS, you're relying on a secure public key cryptographic protocol to shield the information you share with the site from casual eavesdroppers. Public key cryptography underpins most secure communication protocols, including those we use internally at Google as part of our mission to protect our assets and our users' data against threats. Our own internal encryption-in-transit protocol, Application Layer Transport Security (ALTS), uses public key cryptography algorithms to ensure that Google's internal infrastructure components talk to each other with the assurance that the communication is authenticated and encrypted.

Widely-deployed and vetted public key cryptography algorithms (such as RSA and Elliptic Curve Cryptography) are efficient and secure against today's adversaries. However, as Google Cloud CISO Phil Venables wrote in July, we expect large-scale quantum computers to completely break these algorithms in the future. The cryptographic community already has developed several alternatives to these algorithms, commonly referred to as post-quantum cryptography (PQC), that we expect will be able to resist quantum computer-driven attacks. We're excited to announce that Google Cloud has already enabled one of the algorithms on our internal ALTS protocol today.

The PQC threat model

While current quantum computers do not have the capability to break widely-used cryptography schemes like RSA in practice, we still need to start planning our defense for two reasons:

- An attacker might store encrypted data today, and decrypt it when they gain access to a quantum computer (also known as the store-now-decrypt-later attack).
- Product lifetime might overlap with the arrival of quantum computers, and it will be difficult to update systems.

The first threat applies to encryption in transit, which uses quantum vulnerable asymmetric key agreements. The second threat applies to hardware devices with a long lifespan — for example, certain secure boot applications which rely on digital signatures. We focus on encryption in transit in this blog post, as ALTS traffic is often exposed to the public internet, and will discuss the implications for secure boot in our next blog post.

Why we chose NTRU-HRSS internally

With the PQC standards by the National Institute of Standards and Technology (NIST) still pending, rolling out quantum-resistant cryptography can currently only happen on an ephemeral basis, where the exchanged data is used once and never needed anymore. Google's internal encryption in transit protocol, ALTS, is an ideal candidate for such a rollout since we control all endpoints using this protocol and can switch to a different algorithm with relative ease if NIST adopts different standards. Controlling all the endpoints can give us the confidence of defeating store-now-decrypt-later attacks without worrying about having to maintain a non-standard solution.

Deploying new cryptography is risky because it has not been field-tested. In fact, several of the candidates in the NIST process suffered devastating attacks that did not even require a quantum computer. We avoided a scenario where our attempt to secure our infrastructure against a theoretical computing architecture renders it defenseless against a laptop recovering private keys over a weekend by adding the post-quantum algorithm as an additional layer. This tactic helps ensure that the security properties of our currently-deployed vetted and tested cryptography are still in place.

Note that we do not need to address signature algorithms yet. An adversary who can forge a signature in the future will not affect past sessions of the protocol. For now, we only need to address "store now, decrypt later" attacks, as these can affect our data today. Since signature algorithm threats are not immediate, we were able to simplify the vetting process in two ways:

- We only had to add PQC for the key agreement parts of the protocol.
- It allowed us to only change parts which rely on ephemeral keys. For authenticity we still rely on classic cryptography, which likely will only be affected when a large-scale quantum computer exists.

Among the more promising quantum-resistant choices, NIST has favored lattice-based algorithms, with NIST recently announcing the selection of Kyber to become the first NIST-approved post-quantum cryptography key encapsulation mechanism (KEM). Kyber has high performance (it has a more balanced latency cost when considering operations than alternative lattice-based counterparts), but still lacks some clarification from NIST about its Intellectual Property status (see the third round status report by NIST).

From the same realm of lattice-based KEMs, there's the NTRU-HRSS KEM algorithm. This is a direct descendant of the well-known, time-vetted NTRU scheme proposed back in 1996, and it is considered by many experts as one of the more conservative choices among the structured, efficient lattice-based schemes. Given its high performance and maturity, we have selected this scheme to protect our internal communication channels using the ALTS protocol.

The post-quantum cryptography migration brings unique challenges in scale, scope, and technical complexity which have not been attempted before in the industry, and therefore require additional care. That's why we are deploying NTRU-HRSS in ALTS using the hybrid approach. By hybrid we mean combining two schemes into a single mechanism in such a way that an adversary interested in breaking the mechanism needs to break both underlying schemes. Our choice for this setup was: NTRU-HRSS and X25519, thus matching the insightful choice of our Google Chrome 2018's CECPQ2 experiment and allowing us to reuse BoringSSL's CECPQ2 implementation.

Protecting ALTS against quantum-capable adversaries is a huge step forward in Google's mission to protect our assets and users' data against current and future threats. We continue to actively participate in the Post-Quantum Cryptography standardization efforts: Googlers co-authored one of the signature schemes selected for standardization (SPHINCS+), and two proposals currently considered by NIST in the fourth round of their PQC KEM competition (BIKE and Classic McEliece). We may re-evaluate our algorithmic choices when Kyber's IP status is clarified, and when these fourth round selected standards are published.

9.White House Begins To Push Federal Post-Quantum Cryptography Migration

by Alexandra Kelley

https://www.nextgov.com/cybersecurity/2022/11/white-house-begins-push-federal-post-quantum-cryptography-migration/379936/

The White House's Office of Management and Budget released a new memorandum outlining the need for federal agencies' to begin the migration to post-quantum cryptography ahead of the onset of operational quantum computers.

Preparatory measures the OMB recommends federal entities follow the lead of President Joe Biden's earlier executive order enhancing the U.S.'s cyber defense posture. The new memo establishes requirements for federal agencies to inventory their current cryptographic hardware and software systems, emphasizing high value assets and high impact systems that demand extra cybersecurity protocols.

Agency leadership will then be tasked with compiling this information in a report containing their individual summaries on higher risk information assets and systems for the Office of the National Cyber Director and Cybersecurity and Infrastructure Security Agency to help budget, plan, and execute the transition from standard to effective post-quantum cryptography.

OMB officials specify that the high-risk systems submitted by agencies will primarily handle sensitive data that can be exploited by any quantum hacking attempts.

"The Biden-Harris Administration is working to ensure U.S. leadership in the emerging field of quantum computing," Chris DeRusha, the federal chief information security officer, told *Nextgov* in a statement. "This global technology race holds both great promise and threats. We are prioritizing our efforts to secure the Federal Government's sensitive data against potential future compromise by quantum computers; this action signifies the start of a major undertaking to prepare our Nation for the risks presented by this new technology."

Agencies will have until May 4, 2023 to complete OMB's request. Within 30 days of the memo's release, agencies will be tasked with designated a lead for collecting cryptographic systems information. OMB will continue releasing instructions for the collection of the systems inventory.

According to a statement OMB sent to *Nextgov*, the migration to post-quantum cryptographic standards will be the most significant to date, and take several years to complete. Within one year of this new memo's publication, CISA will help release new strategies for migration, in conjunction with the National Institute of Standards and Technology and the National Security Agency.

OMB recommended that as they inventory their information systems, federal agencies should collaborate with software vendors to identify post quantum cryptography testing opportunities within their networks, speaking to the Biden administration's push for public-private sector collaboration.

Several federal agencies have been working in tandem to push the post-quantum migration in government digital networks. NIST previously released four quantum-resistant algorithms to facilitate and expedite updating current code. These will be part of NIST's ongoing Post-Quantum Cryptography initiative, expected to be finalized within two years.

10.Post-Quantum Cryptography Global Markets Gaining Traction

by Dan Yoo

https://www.koreaittimes.com/news/articleView.html?idxno=117339

The U.S. National Institute of Standards and Technology (NIST) announced several candidate Post-Quantum Cryptographic (PQC) algorithms for standardization this summer, and it is nearing the end of a 5-year process. As the final rounds reach their conclusion, global technology intelligence firm ABI Research expects the fledgling PQC market to shift into high gear over the next 5 years as vendors start to fast-track product development plans for commercialization. Global revenues for PQC are expected to grow 12% from 2022 to 2023 and 20% between 2026-2027.

"NIST is the foremost standard development organization leading PQC algorithm development, and much hinges on the successful conclusion of this process, after which work on algorithm integration and the updating of protocols can be advanced by other organizations, industry consortia, and open source movements," says Michela Menting, Cybersecurity Applications Research Director at ABI Research. "The progress of work in these fora will be a sign of technology maturity, and the goal for vendors will be to present "plug and play" types of technologies for their respective industries, making for easier commercial integration and adoption."

Standards and policy recommendations are important drivers for market adoption, stimulating ecosystems, and creating a dynamic and domino effect. They provide the impetus for developing frameworks and timelines around which companies can start strategizing technology integration/migration, creating transition road maps, appointing responsible parties, and allocating dedicated budgets.

The commercial cryptography landscape is set to change radically. The nascent PQC market is already offering many different solutions today, from software libraries to silicon IP and SoC design for semiconductors to initial applications around messaging, VPNs, key management, blockchain, and IoT. Key vendors focused on productizing PQC solutions include niche startups like CryptoNext Security, Crypto Quantique, PQShield, PQ Solutions, Quantropi, and Quantum Xchange as well as established security and technology vendors such as Crypto4A, Entrust, IBM, Thales, and Utimaco, among others.

"To commercialize PQC, vendors still have several challenges to navigate, but the market is ripening, and the first mover advantage will provide lucrative opportunities. First in line are those industries where the lifespan of devices (such as automotive applications) will see the advent of attack-capable quantum computers. Implementing a PQC strategy for those products is imperative today, and the market is quickly positioning itself to deliver on those demands," Menting concludes.

These findings are from ABI Research's Post-Quantum Cryptography application analysis report. This report is part of the company's Cybersecurity Applications research service, which includes research, data, and ABI Insights. Based on extensive primary interviews, Application Analysis reports present an in-depth analysis of key market trends and factors for a specific application, which could focus on an individual market or geography.

11.'Given India's Burgeoning Financial Services Market, There Will Be No Shortage Of Opportunities For Innovative Cryptographic Solutions'

by Sandhya Michu

https://www.expresscomputer.in/cloud/given-indias-burgeoning-financial-services-market-there-will-be-no-shortage-of-opportunities-for-innovative-cryptographic-solutions/91890/

Having established a significant data center presence in Hyderabad and Mumbai, Futurex , a mission-critical data encryption and key-management player looks forward to pursuing new challenges and opportunities within the Indian market, whether they concern cloud or on-premises HSM and key management solutions.

Speaking exclusive to Express Computer, Texas based Adam Cason, Vice President of Global and Strategic Alliances, Futurex talks about the changing payments landscape; especially now that cloud payment HSMs are readily available, including through public cloud marketplaces, organizations are able to fully migrate their payment ecosystem to the cloud

Where do you see maximum adoption of Cloud Payment HSM coming from? What is driving the adoption of Cloud payment HSM services and why?

Within the field of hardware-based security, a steady evolution is taking place. Regulatory requirements mandating the use of strong cryptography are expanding, while many smaller organizations within the financial and tech sectors are looking for ways to secure their applications at a reasonable cost. These factors, as well as general market conditions, are driving a global trend toward increased cloud adoption. However, finance and tech aren't the only markets seeing this increased adoption, which is taking place across several market verticals at once.

What kind of investment is required to create world class Cloud HSM Payment infrastructure? Where does India stand vs the rest of the world in terms of adoption of Cloud Payment HSMs?

India is well known as a global hub for transaction processing and financial services, with thousands of emerging fintechs competing for market share. Cloud solutions are more appealing to these smaller organizations due to the lower cost and faster implementation. However, some hesitancy to adopt cloud solutions can be observed among larger organizations with legacy processing infrastructure. This hesitancy is twofold: on the one hand, migrating legacy infrastructure is a big decision. On the other hand, India's comprehensive data residency laws require organizations to use cloud solutions that are based in India, and that don't store data internationally. In fact, it was in response to this latter obstacle that Futurex established data centers in India to better serve its clients in the region who have need of cloud solutions.

What is your suggestion to CTOs/CIOs/CISOs looking to migrate their payment HSMs?

The biggest obstacles are inertia and compliance, with our solution compliance issues have already been accounted for. Migrating to the cloud is an easy way to reduce costs, both in terms of expenditures and management effort. But an effectively managed cloud solution is the key to maximizing ROI. A trusted vendor can help organizations design and deploy an efficient and well-managed cloud solution that will provide on-demand cryptographic infrastructure for the foreseeable future.

Where do you see Cloud Payment HSM in India 5 years down the line? What according to you can be done to further boost Cloud Adoption in the country?

In establishing data centers throughout India, Futurex took the necessary first steps to provide organizations in the region with powerful and efficient cloud solutions. We've seen success with this initiative and expect that trend to continue. But markets are big ships to turn; while cloud adoption may not storm the market overnight, it will inevitably gain traction as companies see the returns in their cloud investments.

What are Futurex's offerings in the payment HSM and Cloud Payment HSM space? Please elaborate your plans for the market.

Futurex has been developing, manufacturing, and implementing payment HSM technology for over 40 years. We currently have customer-focused cryptographic solution suite, comprising HSMs for payments and general-purpose encryption, key management servers, and infrastructure management tools. Our solutions can be deployed on-premises as well as through our VirtuCrypt cloud platform. What sets our solutions apart is their near-universal support for different APIs, cryptographic algorithms, and international compliance standards.

What has been the journey of the company in India? Could you share your existing business model?

For over 40 years, Futurex has remained the trusted global provider of hardened enterprise-class data security solutions. Over 15,000 business and financial organizations use the company's innovative cryptography and tokenization solutions to address mission-critical data encryption and key-management needs. Futurex has long-running partnership throughout India, including both payment solutions providers, channel distributors, and resellers. When we established a significant data center presence in Mumbai and Hyderabad, it was with the intention of bringing our innovative solutions to an already fast-growing market in need of fresh options.

How do Cloud Payment HSMs work? What are their advantages over on-premises payment HSM?

Cloud HSMs use the technological framework of physical HSMs to deliver the same cryptographic functionality and level of security through a cloud platform. The advantages in cloud payment HSMs lies in the on-demand agility of the cloud, as well as its relatively lower cost to entry: cloud payment HSM solutions are fairly simple to deploy and can be scaled according to need.

With cloud-based encryption and key management accelerating, we'll see more payment processing in the cloud. What are some of the challenges and opportunities you see for your business?

Between Futurex's industry-leading technology, highly knowledgeable sales team, and tried-and-true support staff, all of whom are accustomed to international markets, we are fairly well versed in taking on new challenges. In the Indian market, these challenges present themselves more as opportunities, with larger enterprises deciding whether to refresh their legacy infrastructures with on-premises hardware or cloud HSM solutions, and smaller organizations like fintechs searching for affordable yet robust security cloud services. Fortunately, Futurex's solution suite is versatile enough to accommodate these needs, and our local data center presence makes cloud solutions more viable than ever.

12.Quantum Cryptography Apocalypse: A Timeline And Action Plan

by Konstantinos Karagiannis

https://www.darkreading.com/attacks-breaches/quantum-cryptography-apocalypse-a-timeline-and-action-plan

There is a potential dark side to quantum computing, one that is a threat to how we secure data. Back in 1994, Peter Shor developed an algorithm for factoring large numbers using a quantum computer, which could be used to break encryption. Today, RSA encryption relies on the difficulty a classical computer has with such factorization. With Shor's algorithm in mind, nation-states and nefarious actors started harvesting data packets, dreaming of a future where they would be able to decrypt those packets using a fault-tolerant quantum computer.

Currently, there are about three dozen quantum computers in the cloud. These quantum computers are error-prone and lack enough quantum bits (qubits) to run Shor's algorithm against RSA encryption. Some experts claim quantum computing will not be a threat for at least 30 years. However, those claims may be based upon outdated information and there is evidence that quantum computing will have the power to crack encryption sooner than we thought.

Identifying Quantum Threats

The day is coming when a quantum threat (Y2Q) to encryption becomes a reality. Y2Q proves similar to a combination of the Y2K bug and the 2014 Heartbleed attack, where it will affect almost every system on the planet and severely affect data in motion.

Y2Q affects two types of general cryptography: symmetric and asymmetric. Symmetric encryption is used for data at rest and functions like a locked box with a key. Shor's algorithm cannot attack symmetric encryption ciphers such as AES, however Grover's search algorithm can weaken it. To combat Y2Q in this situation, we can increase the symmetric key size and make it even more difficult to attack via brute force.

Data in motion on a network is protected by asymmetric encryption, which is commonly called public key cryptography, and its most prevalent example is via a cipher known as RSA. RSA is vulnerable to Shor's algorithm, allowing a quantum computer to reverse private keys and read messages. Blockchain also uses a type of public key encryption called ECC, which means the crypto economy is also threatened by quantum computing.

Preparing for Y2Q begins with conducting a post-quantum crypto (PQC) agility assessment. Crypto agility is the ability to introduce new cryptography to an organization's hardware and software without being disruptive to infrastructure. However, identifying those primary threats is not easy. It is a matter of determining what ciphers are used throughout an organization, including in third-party hardware and software. Further complicating the process is that some elements may not have a path forward for post-quantum cryptography.

Exploring the PQC Threat and Timeline

It may be too late to protect certain types of data. Mosca's theorem states that you must add the number of years it takes your organization to migrate to new cryptographic standards and primitives to the shelf life of your secret. For example, three years to migrate plus a regulatory requirement of 10 years of maintenance would equal 13 years.

Using the implementation example of Shor's algorithm called Toffoli-based modular multiplication, we can estimate that quantum computers will have enough power (high-fidelity qubits) to crack encryption by the end of this decade.

However, the quantum world is constantly making observations on its denizens, including qubits, which causes them to decohere and become "classical" or unable to compute with quantum algorithms. System builders must account for this noise and resolve engineering challenges to make qubits near perfect with 99.99% fidelity. We also need to run error correction, which requires sacrificing some physical qubits to create a logical, error-corrected qubit.

Qubit growth can be accelerated by using a few modest-size, quality quantum computers that work together using a technology called interconnect, which allows quantum computers to entangle qubits to behave as one quantum computer. If we get interconnect right, we could take, say, four 1,100-qubit quantum computers and instantly have a 4,400-qubit machine capable of doing damage to encryption.

IBM has a grim prediction that it will take 1,000 physical qubits to yield one error-corrected qubit. However, IonQ thinks it is closer to 16 to 1. An estimate between those two extremes indicates that if we get close to 1 million physical qubits this decade, we will quickly surpass current predictions.

NIST is aware of the looming threat and has been working to develop a new standard of PQC with ciphers to replace RSA. We expect a new standard by the end of 2024.

In May 2022, the White House released the National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. That memo has action demands on federal entities to be taken after NIST finalizes the new standard.

We can expect regulators and other industries in the private sector to mirror these expectations closely. Simply put, organizations must become crypto-agile and introduce hybrid PQC solutions for today's most critical data flows.

13.The Top Five Cybersecurity Trends In 2023

by Bernard Marr

https://www.forbes.com/sites/bernardmarr/2022/11/11/the-top-five-cybersecurity-trends-in-2023/?sh=5198e5481785

In recent years we have seen the topic of cyber security move from the IT department to the board room. As attacks have proliferated and the potential penalties, both regulatory and in terms of loss of customer trust, have increased, it has become a priority at every organizational level.

We often think of cybersecurity as an ongoing battle between hackers and criminals, and security experts, which is constantly escalating due to constant advances in technology. This is the “glamorous” side of the business that we sometimes see depicted in TV shows and movies. And indeed, threats sometimes come from hostile foreign states or devious, tech-savvy criminal masterminds. In reality, however, threats are just as likely to emerge due to improperly secured networks leaving sensitive data accidentally exposed, or unwary or indiscreet employees using non-secured devices while working from home.

A shift to a culture of home and remote working that started during the Covid-19 pandemic and has persisted in many organizations, as well as the spread of the internet of things (IoT) into every area of business and society, means there has never been more opportunity for lax security to cause headaches and expense. Because of this, cybersecurity is top of everyone's agenda in 2023, so here's a look at some of the key trends in 2023:

Internet of Things and cloud security

The more devices we connect together and network, the more potential doors and windows exist that attackers can use to get in and access our data. And in 2023, analysts at Gartner predict, there will be 43 billion IoT-connected devices in the world.

IoT devices – ranging from smart wearables to home appliances, cars, building alarm systems and industrial machinery – have often proven to be a bugbear for those with responsibility for cybersecurity. This is because, as they are often not used to store sensitive data directly, manufacturers haven't always been focused on keeping them secure with frequent security patches and updates. That has changed recently, as it's been shown that even when they don't store data themselves, attackers can often find ways to use them as gateways to access other networked devices that might. Today, for example, you're less likely to find a device shipped with a default password or PIN that doesn't require the user to set their own, as was frequently the case in the past.

In 2023, a number of governmental initiatives around the world should come into effect designed to increase security around connected devices, as well as the cloud systems and networks that tie them all together. This includes a labeling system for IoT devices set to be rolled out in the US to provide consumers with information on possible security threats posed by devices they bring into their homes.

Work-from-home cybersecurity becomes a priority for businesses

Recently, a cybersecurity priority for many organizations has been to secure the millions of devices worldwide that are being used for home and remote working since the start of the pandemic. Pre-pandemic, when we were all office-based, it was simple enough for security agents, probably based in IT departments, to regularly check and update company laptops and smartphones. This made it relatively simple to ensure they were free of spyware and malware and were running the latest versions of antivirus software and other preventative measures. In 2023, when workers are more likely than ever to use personal devices to remotely connect to work networks, a new set of challenges has emerged.

Connecting to networks with non-secured devices can lead to employees unwittingly falling victim to phishing attacks, where attackers trick users into divulging passwords. With more people working remotely, it's increasingly likely we may find ourselves working in teams where we don't know each other as well and are at risk of falling for impersonation scams. It also enables ransomware attacks, where software is injected into networks that erase valuable data unless users pay a ransom to attackers. The risk of this also increases in remote working situations, where it's more likely that devices may be left unattended.

International state-sponsored attackers target businesses as well as governments

Nation-states frequently take part in cyber-espionage and sabotage in an attempt to undermine unfriendly or competing governments or to access secrets. In this day and age, however, it's increasingly likely that companies and non-governmental organizations (NGOs) will find themselves targeted by state actors.

Since the 2017 WannaCry ransomware attack, believed to have been perpetrated by hackers affiliated with the government of North Korea, there have been hundreds of thousands of attacks on servers all around the world that security agencies believe can be traced to foreign governments.

In 2023, more than 70 countries are due to hold governmental elections – events that are frequently a target for attack by hostile foreign interests. As well as hacking and cyberattacks on infrastructure, this will take the form of disinformation campaigns on social media. This often involves seeking to influence the results in favor of political parties whose victories would benefit the government of the hostile state. And cyber warfare will undoubtedly continue to form a key element in armed conflict, with one analyst saying of the Russia-Ukraine war that “Digital is an important a part of this war as is the fighting on the ground.”

Artificial intelligence (AI) plays an increasingly prominent role in cybersecurity

As the number of attempted cyberattacks has grown rapidly, it has become increasingly tricky for human cybersecurity experts to react to them all and predict where the most dangerous attacks will take place next. This is where AI comes into play. Machine learning algorithms can examine the vast amount of data moving across networks in real-time far more effectively than humans ever could and learn to recognize patterns that indicate a threat. According to IBM, companies that use AI and automation to detect and respond to data breaches save an average of $3 million compared to those that don’t.

Unfortunately, thanks to the ever-growing availability of AI, hackers, and criminals are growing increasingly proficient at using it too. AI algorithms are used to identify systems with weak security or that are likely to contain valuable data among the millions of computers and networks connected to the internet. It can also be used to create large numbers of personalized phishing emails designed to trick receivers into divulging sensitive information and become increasingly good at evading automated email defense systems designed to filter out this type of mail. AI has even been used to artificially “clone” the voice of senior executives and then to fraudulently authorize transactions!

This is why the use of AI in cybersecurity is sometimes referred to as an "arms race," as hackers and security agents race to ensure the newest and most sophisticated algorithms are working on their side rather than for the opposition. It’s been predicted that by 2030 the market for AI cybersecurity products will be worth close to $139 billion – a near tenfold increase on the value of the 2021 market.

Building a security-aware culture

Perhaps the most important step that can be taken at any organization is to ensure that it is working towards initiating and fostering a culture of awareness around cybersecurity issues. Today, it’s no longer good enough for employers or employees to simply think of cybersecurity as an issue for the IT department to take care of. In fact, developing an awareness of the threats and taking basic precautions to ensure safety should be a fundamental part of everyone’s job description in 2023!

Phishing attacks rely on “social engineering” methods to trick users into divulging valuable information or installing malware on their devices. No one needs technical skills to learn to become aware of these types of attacks and to take basic precautions to avoid falling victim. Likewise, basic security skills like the safe use of passwords and developing an understanding of two-factor authentication (2FA) should be taught across the board and continually updated. Taking basic precautions like this to foster a culture of cybersecurity-awareness should be a core element of business strategy at organizations that want to ensure they build resilience and preparedness over the coming 12 months.

14.Developing Cryptographic Technologies In Blockchain

https://www.hardwaretimes.com/developing-cryptographic-technologies-in-blockchain/

Companies must maintain secure and reliable relationships with suppliers, distributors, and trading partners worldwide. With a small initial deposit, platforms like the **bitcoin code app** offer the best bitcoin trading experience. The withdrawals on this platform are quick with extraordinary security. They also have to make sense of the information provided by blockchain projects increasingly becoming a part of everyday operations.

In response to these complex needs, major financial institutions, tech companies, and governments are all developing cryptography technologies in the blockchain. These developments can help you become better informed about how your company deals with customers and competitive businesses – or maybe even find new opportunities. Cryptography in Blockchain: The Basics

Humans have used cryptography for thousands of years to protect trade secrets, military strategies, and sensitive diplomatic communications. However, modern cryptography relies on mathematical functions that are incredibly difficult – or even impossible – to reverse. In the blockchain, public-key cryptography (or asymmetric cryptography) is used to secure transactions and validate interactions between participants.

While an everyday private-public key pair in the blockchain is an identity, the same key pairs can be used for encryption (e.g., securing sensitive information).   For example, a blockchain network might exchange public keys with potential trading partners so they can securely send trade offers to the network.

Cryptography in Blockchain: How it Works

Only the private decryption key, which must remain secret, can unlock encrypted data. Hashing involves encrypting information by running it through a one-way function. The resulting string of characters is then stored in the blockchain. Zero-knowledge proofs are often used to verify transactions in blockchain networks with anonymous participants. For example, an online marketplace can use zero-knowledge proof cryptography to ensure that buyers receive their orders without revealing their identities or credit card numbers to sellers' computers/networks.

Avalanche effect:

The Avalanche effect is used to block miners from creating blocks on top of other blocks, i.e., ensuring that the network will not accept a block added in the middle of the chain. To understand this, consider how these transactions are broadcast to the network:

The nodes collect all transactions in a temporary memory which is called Manolo. Each node then picks the transactions from this pool, puts them into a new block, and then tries to hash them. These transaction blocks are sent to other nodes for verification, and if any node finds that block invalid, it will reject it.

Cryptographic hash functions provide the following benefits to the blockchain:

- **Immutable** – Unlike a digital signature, which can be modified and changed to deceive others, cryptographic hash functions are hard to change and easy to verify.
- **Consistent** – Consistent hashing ensures that no two transactions in the blockchain contain the same hash.
- **Secure** – Cryptographic hash functions are among the most secure methods available to transmit sensitive information – and, therefore, should be used whenever any transaction involves sensitive fields like credit cards or your personal information.

15.SES Selects Arianespace To Launch EAGLE-1 Satellite For Europe's Quantum Cryptography

https://www.arianespace.com/press-release/ses-selects-arianespace-to-launch-eagle-1-satellite-for-europes-quantum-cryptography/

The EAGLE-1 satellite, which will support the end-to-end secure Quantum Key Distribution (QKD) system for Europe, will be launched for SES by Arianespace on a Vega C rocket from French Guiana as early as Q4 2024. The satellite will be placed into Low Earth Orbit (LEO). The EAGLE-1 project comprising satellite and ground infrastructure, is developed by SES and its consortium of 20 European partners, with the European Space Agency (ESA) and the European Commission support.

Under the recently-signed agreement with ESA, SES and its partners will design, develop, launch and operate a satellite-based end-to-end QKD system for the purpose of testing and validating space-based secure transmission of cryptographic keys. The first European sovereign space-based QKD system will include the dedicated low earth orbit (LEO) EAGLE-1 satellite and state-of-the-art QKD operations centre in Luxembourg. In the scope of EuroQCI, the EAGLE-1 satellite will enable early access, validation, and integration of space-based QKD for EU Member States.

“Building the EAGLE-1 end-to-end system for secure data transmission and validating the long-distance Quantum Key Distribution technology is an innovative project that will benefit the EU Member States,” said Ruy Pinto, Chief Technology Officer at SES. “We have been working with Arianespace for decades to deliver our satellites into space and are delighted for them to be onboard to launch the EAGLE-1 satellite into orbit.”

“We are delighted and honored by this renewed mark of confidence from the leading global content connectivity service provider SES,” noted Marino Fragnito, director of Arianespace’s Vega business unit. “Over the last 38 years, we have carried out 42 launches for our longstanding partner, and Vega C will now continue this successful track record. It is a great honor for us to support our customer ambitions and to be part of this mission that aims at implementing Europe’s satellite-enabled cybersecurity technology.”

Following the launch, the EAGLE-1 satellite will complete three years of in-orbit mission supported by the European Commission. During this operational phase, the satellite will allow European Union governments and institutions, as well as critical business sectors, early access to long-distance QKD that would path the way towards an EU constellation enabling ultra-secure data transmissions.

The EAGLE-1 project is co-funded by the ESA contribution of Germany, Luxembourg, Austria, Italy, the Netherlands, Switzerland, Belgium, and the Czech Republic under ARTES, as well as the European Commission through Horizon Europe.

Vega C, the new European light launcher, successfully passed its inaugural flight on July 13 and now enters its operational phase under the responsibility of Arianespace. With this contract, Vega C backlog includes over 40 satellites contracts.

Vega C development program has been managed by ESA with 12 Member States of the Agency. Avio Spa (Colleferro, Italy) is the industrial prime of the Vega launch system. Vega C has been upgraded with more powerful first and second stage Solid Rocket Motors and with a larger fairing, which significantly increases payload mass and double allowable volume as compared to Vega. The launcher also better meets the specific needs of small spacecraft, thanks to its improved SSMS dispenser and to its AVUM+ that allows seven re-ignitions instead of five. Vega C can thus deliver to three different separation orbits for its multiple payloads within the same mission, instead of the two previously possible with Vega.

16.Can Post-Quantum Encryption Save The Internet?

by Greg Noone

https://techmonitor.ai/technology/emerging-technology/post-quantum-encryption-threat-already-here

The future of privacy online begins and ends with the demise of public key cryptography. Mathematical riddles shared between two nodes in a network, modern encryption techniques would take trillions of years for your everyday ‘classical’ computer to crack. Quantum computers, meanwhile, will make short shrift of these conundrums. Machines capable of harnessing the mysteries of quantum mechanics to achieve feats of computation vastly superior to its silicon-based antecedents, the announcement that a quantum computer had broken RSA, DES or AES would render vast swathes of the internet insecure overnight.

This moment is often referred to by cryptographers as ‘Q-Day,’ though when it’ll arrive is anyone’s guess. Some predict it’ll take as little as eight years before conventional cryptography will be broken by a quantum computer, while others insist we still have a few decades before any quantum advantage well and truly breaks the internet. According to mathematicians like Dustin Moody, however, we may not even know the precise moment when conventional encryption is cracked. “It could be that it’s happening behind the scenes and we don’t know it for a while,” says the mathematician and expert in all things quantum at the US National Institute for Standards and Technology (NIST.)

It’s the reason why Moody and his colleagues at NIST have been holding a competition since 2016 to source new standards for encryption algorithms that, in theory, should be able to withstand the code-breaking abilities of mature quantum computers. “We wanted to make sure we have standards ready as soon as possible, even though a quantum computer is still off in the future,” says Moody. After multiple rounds of testing, both inside the organisation and at the hands of external cryptographers, NIST announced its approval in July of four algorithms it believes are quantum-safe for the purposes of encryption and digital signatures, with another four placed ‘under consideration’.

Eventually, these post-quantum encryption algorithms will supplant their RSA and DES equivalents – a more elegant solution, experts like IBM’s Scott Crowder argue, than quantum key distribution (QKD), which harnesses the mysteries of quantum mechanics to physically secure communications but requires massive investment in new ground infrastructure and satellites. “From our perspective, it’s not necessary or sufficient to really make you secure against quantum computers,” says the firm’s vice-president for quantum adoption.

There’s only one problem: post-quantum encryption algorithms keep being broken by classical computers. This happened as late as this summer, when one of the algorithms under consideration by NIST was broken by two Belgian cryptographers in just a couple of hours using only a laptop. Moody is well aware of the consequences in taking a wrong turn on these standards, even though a quantum computer capable of breaking RSA is arguably decades away from being built. Even so, he says, the threat posed by ‘harvest now, decrypt later’ attacks, wherein encrypted data is trawled by hackers and stowed away until it can be cracked open by a quantum machine, is very real.

“Most data these days has a pretty good lifespan,” explains Skip Sanzeri, founder of quantum startup QuSecure. “Think of personal information: that can be 50 to 75 years, depending upon a lifetime. Healthcare information? Usually over 50 years. Banking information? 25 years. Military secrets? 75 years.” The integrity of all of those secrets, argues Sanzeri, is therefore threatened in the here and now – regardless of when a quantum computer gets round to decrypting it.

How to write post-quantum encryption algorithms

The emergence of the post-quantum threat signals the end of what was an effective solution to the problem of securing information online. Devised in the 1970s, modern encryption methods require pairs of classical computers to parse mathematical problems that can only be solved with helpful pre-existing clues, known as ‘keys’, which are only available to the machines.

In the case of RSA, that involves prime factorization, or the act of factorizing large-enough integers of a number into its component primes. If one computer in the communicating pair already has the primes ready, it takes them no time at all. This is known as the ‘private key,’ while the ‘public key’ is the product of the primes. Only once both are produced can the encrypted message be unlocked.

Absent these keys, a classical computer would spend years – 300 trillion of them, according to one estimate – trying to work out a single prime factorization problem. However, in 1994, a researcher named Peter Shor devised a new algorithm that demonstrated how a quantum computer might harness the superimposed quantum status of its component informational units – known, in short, as qubits – to crack encryption methods like RSA in next to no time at all. “It’s really just because of Shor’s algorithm that quantum computers are relevant,” says Moody.

All that remained, then, was to build the machine. In 1998, that work began with the creation of a 2-qubit quantum computer at Oxford University. The number of working qubits has edged slowly upward in the intervening decades, which has also served to increase anxiety among cryptographers looking for a form of encryption immune to quantum attack. Boiled down, says Crowder, this involved “trying to find a math problem that both classical computers and quantum computers suck at”.

Experts believe that quantum computers could crack conventional encryption within two decades

The hardest puzzle to solve in this regard seems to be lattice-based cryptography. Devised in the 1980s, this method’s strength lies in how difficult it is to calculate the nearest point between one number and another in a lattice structure encompassing up to 500 separate spatial dimensions. Four of the quantum-safe algorithms NIST eventually chose to recommend for standardisation, in both encryption and digital signatures, were lattice-based. “They’re good, all-round performers,” says Moody. “They’re very efficient. Their key sizes are not too big. Their security has been well-studied.”

It's been a long and painful process to get to those final four. Early examples of lattice-based encryption were difficult to parse for classical computers, even with access to the necessary public keys, leading cryptographers to simplify the algorithms and inadvertently compromise their security. It's a pattern that's persisted into the present day, with dozens of examples volunteered for NIST's evaluation being compromised since 2016. "In the first round, there were probably 15 to 20 that got broken," says Moody. "In the second round, there were seven. And even in the third round... Rainbow was broken, and then, more recently, SIKE was also broken."

Additionally, without an actual quantum computer to hand, there's no guarantee that the algorithms which survived NIST's third round are truly quantum-safe. Until then, says Moody, we don't really have a choice but to trust in the Darwinian process of winnowing out the weakest algorithms by open-sourcing their code and watching them get picked off, one by one, by the wider cryptographic community.

"This is how we gain confidence," says Moody. "We put them out there for the expert to evaluate; we give them a number of years to look at them; and, if a lot of people look at it and over a number of years, nobody finds any weaknesses, we can start to gain confidence in them."

Preparing businesses for post-quantum encryption

It remains uncertain how long Moody and the rest of the cryptographic community will have to scrutinise these post-quantum encryption algorithms. Sanzeri is among the corps of true believers in the quantum community who think it likely that a machine capable of cracking RSA encryption by the end of this decade. And by that point, he adds, their ability to compute variables in problems at the drop of a hat means that a spot of codebreaking will be the least of its accomplishments.

"That's why," says Sanzeri, "they're going to be awesome for AI, genomics and protein folding, chemistry, material science, optimisation, logistics, aerospace design - things where you've got tons and tons and tons of variables."

Others in the field are more sceptical. A study published earlier this year estimated that it would take 13 million qubits to crack 256-bit encryption in a day - or, if you were in more of a rush, 317 million in an hour. By comparison, one of the most advanced quantum processors in existence, IBM's 'Osprey' processor, has just 433 qubits. Although there is a clear roadmap to increasing the computational power of a quantum computer by parallelizing these processors, these devices will require significant assistance from error-correction algorithms to run in a useful way, says one of the study's authors, Dr Sebastian Weidt - a research field, he adds, which is extremely nascent.

Regardless of when a code-cracking quantum computer is actually built, though, Weidt is adamant that businesses should be preparing for the post-quantum future now. "You'd love to think that, because we're shouting this message very loudly years in advance, that it's [going to be] barely a footnote somewhere that this has happened," he says. "But realistically, lots of people will get caught out."

Some might have been already. Both the UK's National Cyber Security Centre and the NSA have been highly vocal in recent years about the need to secure telecommunications networks from quantum attacks, while both Sanzeri and Moody claim to have heard furtive whispers from their own contacts in the intelligence community that HNDL attacks are probably already happening.

As such, several institutions have already begun preparing for the post-quantum future, led first and foremost by the US government. In May, the Biden administration ordered federal agencies to begin preparing plans to secure their networks using post-quantum encryption algorithms, in addition to directing NIST to establish a working group to prepare the private sector for the road that lies ahead. They'll be working alongside a growing number of start-ups like QuSecure and various tech giants that offer their own post-quantum preparation services.

“Those big companies – the Google’s, Microsoft, IBM, Intel – they’re all very well aware of the quantum threat,” says Moody. “As soon as the standards come out, you’ll see them start using the algorithms in their products.”

Some multilaterals, like Mastercard, have started offering products utilising quantum cryptography as a way of signalling their security credentials. IBM, meanwhile, is liaising with a range of banks, telecoms providers and manufacturers to harden their networks against quantum attack. “If you look at it from Vodafone’s perspective, they are a player that has a lot of their own IT, but they rely on a whole mass of vendors in their supply chain,” says Crowder. For their systems to be truly secure, he adds, their vendors need to be hardened against quantum attacks as well. “It’s an ecosystem play.”

Crowder is under no illusions, however, that transitioning such systems will be easy. “We definitely had to upgrade SHA-1, SHA-2, SHA-3, over time,” he says. “But we’ve never, since the internet got launched, really, had to do a transformation of this nature.”

Meanwhile, the world awaits NIST’s final judgement about post-quantum encryption standards. For his part, Moody expects those to be published next year. But, he adds, businesses shouldn’t wait to ready themselves for what lies ahead. “Learn all you can,” says Moody. “Talk to us if you have questions – and make sure your organisation is prepared for this quantum threat.”

17.IBM Unveils 400 Qubit-Plus Quantum Processor And Next-Generation IBM Quantum System Two

by Hugh Collins & Chris Nay

https://techmonitor.ai/technology/emerging-technology/vodafone-quantum-cryptography-ibm

IBM today kicked off the IBM Quantum Summit 2022, announcing new breakthrough advancements in quantum hardware and software and outlining its pioneering vision for quantum-centric supercomputing. The annual IBM Quantum Summit showcases the company's broad quantum ecosystem of clients, partners and developers and their continued progress to bring useful quantum computing to the world.

"The new 433 qubit '**Osprey**' processor brings us a step closer to the point where quantum computers will be used to tackle previously unsolvable problems," said Dr. Darío Gil, Senior Vice President, IBM and Director of Research. "We are continuously scaling up and advancing our quantum technology across hardware, software and classical integration to meet the biggest challenges of our time, in conjunction with our partners and clients worldwide. This work will prove foundational for the coming era of quantum-centric supercomputing.”

At the Summit, the company unveiled the following new developments:

- **‘IBM Osprey’ - IBM’s new 433-quantum bit (qubit) processor**

  IBM Osprey has the largest qubit count of any IBM quantum processor, more than tripling the 127 qubits on the IBM Eagle processor unveiled in 2021. This processor has the potential to run complex quantum computations well beyond the computational capability of any classical computer. For reference, the number of classical bits that would be necessary to represent a state on the IBM Osprey processor far exceeds the total number of atoms in the known universe. For more about how IBM continues to improve the scale, quality, and speed of its quantum systems, read Quantum-Centric Supercomputing: Bringing the Next Wave of Computing to Life.

New quantum software addresses error correction and mitigation

Addressing noise in quantum computers continues to be an important factor in adoption of this technology. To simplify this, IBM released a beta update to Qiskit Runtime, which now includes allowing a user to trade speed for reduced error count with a simple option in the API. By abstracting the complexities of these features into the software layer, it will make it easier for users to incorporate quantum computing into their workflows and speed up the development of quantum applications. For more details read Introducing new Qiskit Runtime capabilities — and how our clients are integrating them into their use cases.

IBM Quantum System Two update – IBM's next-generation quantum system

As IBM Quantum systems scale up towards the stated goal of 4,000+ qubits by 2025 and beyond, they will go beyond the current capabilities of existing physical electronics. IBM updated the details of the new IBM Quantum System Two, a system designed to be modular and flexible, combining multiple processors into a single system with communication links. This system is targeted to be online by the end of 2023 and will be a building block of quantum-centric supercomputing — the next wave in quantum computing which scales by employing a modular architecture and quantum communication to increase its computational capacity, and which employs hybrid cloud middleware to seamlessly integrate quantum and classical workflows.

- **New IBM Quantum Safe technology:** As quantum computers grow more powerful, it is crucial that technology providers take steps to protect their systems and data against a potential future quantum computer capable of decrypting today's security standards. From offering the z16 system with quantum safe technology, to contributing algorithms in connection with the National Institute of Standards and Technology's (NIST) goal for standardization by 2024, IBM offers technology and services with these security capabilities. At the Summit, IBM and Vodafone announced a collaboration to explore how to apply IBM's quantum-safe cryptography across Vodafone's technology infrastructure.

- **Client & Ecosystem Expansion**: Growth of IBM Quantum Network: IBM also announced today that German conglomerate Bosch has joined the IBM Quantum Network to explore a variety of quantum use cases. Other recent additions to the network include multinational telco Vodafone to explore quantum computing and quantum-safe cryptography, French bank Crédit Mutuel Alliance Fédérale to explore use cases in financial services, and Swiss innovation campus uptownBasel to boost skill development and promote leading innovation projects on quantum and high-performance computing technology. These organizations are joining more than 200 organizations — and more than 450,000 users — with access to the world's largest fleet of more than 20 quantum computers accessible over the cloud.

"The IBM Quantum Summit 2022 marks a pivotal moment in the evolution of the global quantum computing sector, as we advance along our quantum roadmap. As we continue to increase the scale of quantum systems and make them simpler to use, we will continue to see adoption and growth of the quantum industry," said Jay Gambetta, IBM Fellow and VP of IBM Quantum. "Our breakthroughs define the next wave in quantum, which we call quantum-centric supercomputing, where modularity, communication, and middleware will contribute to enhanced scaling computation capacity, and integration of quantum and classical workflows."

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

18.Vodafone Partners With IBM On Quantum-Safe Cybersecurity

by Ryan Morrison

https://techmonitor.ai/technology/emerging-technology/vodafone-quantum-cryptography-ibm

Telecoms giant Vodafone is working with IBM to secure its network against the risk of future quantum computers that could crack existing cryptography including public key encryption. The deal will also provide Vodafone engineers with cloud access to IBM's quantum computing hardware.

Today's quantum computers are not able to crack cryptographic keys as they don't have enough processing power to work through the complex mathematical problems used to secure data. However, most experts predict it will happen within the next decade or two.

It all comes down to multiplication. Today's standards use problems that are easy for a computer to verify but difficult to solve. A classical computer struggles with factors of large numbers but can easily check two prime numbers multiply together to some large numbers. Modern encryption makes use of very large numbers as codes in a way their prime factors form the key but this isn't going to be a complex problem for fault-tolerant quantum computers.

Some experts say a quantum computer with millions of qubits, or quantum bits, will be required before it can become fault-tolerant enough to crack these complex problems. Researchers from the University of Sussex predict it will take more than 317 million qubits to crack 256-bit elliptic curve encryption with a quantum computer in an hour, and a 13 million qubit machine to crack it in a day.

IBM announced today that its 433-qubit Osprey quantum computer was fully operational, and revealed plans for its next generation of modular quantum supercomputing called System 2, with more than 4,000 qubits by 2025. So there is some time to go before it can crack the code.

Cryptography and beyond

The machines will get there and as replacing encryption across all devices and nodes within a network can take a long time, as can developing quantum-safe algorithms, the race is on. Governments, industry and researchers are spending billions developing new standards that are quantum-safe, also known as post-quantum cryptography.

The new partnership with Vodafone was announced during the IBM Quantum Summit, where it was also confirmed Vodafone will work with IBM to help validate and progress potential quantum use cases in telecommunications beyond just cryptography.

Vodafone will explore quantum computing and its impact on a variety of telecom industry use cases as well as train employees on the technology through an 'iterative prototyping' project led by IBM. It will also go on a recruitment drive to find quantum computing experts.

19.Xiphera And Flex Logix Publish Joint White Paper On Solving The Quantum Threat With Post-Quantum Cryptography On EFPGA

https://www.prnewswire.com/news-releases/xiphera-and-flex-logix-publish-joint-white-paper-on-solving-the-quantum-threat-with-post-quantum-cryptography-on-efpga-301670139.html

Xiphera Ltd, a Finnish company designing and licensing cryptographic IP cores for FPGAs and ASICs, announced today that it has published a new white paper with Flex Logix, the leading supplier of eFPGA IP. The paper explains how advances in quantum computing technology threaten the security of current cryptosystems and how this can be averted with Post-Quantum Cryptography (PQC) running on embedded FPGAs (eFPGAs.)

While quantum computing and its development offer answers to various computational problems, they also threaten the security of current cryptosystems. PQC systems respond to this growing quantum threat because they are based on mathematical problems that cannot be solved efficiently with Shor's algorithm, or by any other known quantum computing algorithm. When PQC is implemented on eFPGA, it can provide the crypto agility that customers need to change the PQC algorithms, yet provide the performance, power and cost savings over other alternatives.

"PQC is expected to happen within the next few years, so companies developing chips that need to be operational for 10+ years, should build in crypto agility in their chips today," said Kimmo Järvinen, Co-Founder and CTO of Xiphera. "Using eFPGA as implementation platforms for PQC enables a smooth and secure shift from traditional cryptosystems to the new PQC systems."

"SoC designers need the ability to change algorithms as needed without sacrificing power and cost savings to address algorithms evolving over time," said Andy Jaros, VP of Sales for Flex Logix. "If PQC is implemented on an eFPGA platform, then all forthcoming updates and algorithm modifications can be supported by simply reprogramming eFPGA. In addition, it is also possible to retro-fit PQC into systems that already have eFPGA included in the SoC."

Details on the White Paper

Many organizations and associations will require PQC support on security systems in the near future. However, these requirements and the continuously changing PQC landscape requires a new level of crypto agility and the ability to update and change cryptographic algorithms in deployed systems.

The white paper discusses implementation of PQC algorithms on eFPGA and how this can deliver tremendous advantages to SoC designers. Not only can it allow the updating of PQC algorithms according to their development status, but it also enables designers to combine PQC with traditional cryptosystems and existing crypto modules in order to protect against unlikely but possible failures of the new PQC systems.

20.Competition Between China & Us Fuelling Growth Of The Quantum Ecosystem, Says Sabrina Maniscalco

by James Dargan

https://thequantuminsider.com/2022/11/04/competition-between-china-us-fuelling-growth-of-the-quantum-ecosystem-says-sabrina-maniscalco-co-founder-ceo-of-algorithmiq/?utm_source=newsletter&utm_medium=email&utm_term=2022-11-26&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+ColdQuanta+s+Serious+Series+B+Quantum+Is+Online+in+Finland+And+More+Quantum+News

Global Frontrunner

In an excellent article published in Fortune in September, The U.S., China, and Europe are ramping up a quantum computing arms race. Here's what they'll need to do to win, the writers give their view on which country will come out on top.

As expected, they believe the US *is* and *will* be "the global frontrunner", though China will certainly be "breathing down its neck".

Closer to home, The Quantum Insider (TQI) recently published an insightful piece by Anders Liman, a graduate student studying Tech Ethics and Science Policy at Duke University and a Tech Policy Researcher at the Responsible AI Institute.

In Competing Interests, Competing Ideals, and Unwanted Hype in Quantum Computing, and ways to Address Them: Global Quantum Computing Policy, Liman focused on competing interests and ideals:

The challenge of competing interests is further heightened when there are competing ideals. This is more likely to occur internationally. It may happen between two nations that value democracy or intellectual property to differing degrees. It may also happen between two nations who see the government's role in scientific innovation differently.

It's obvious who he's talking about.

Maniscalco Talks

This topic again came up during the week at the Websummit in Lisbon, Portugal. Sabrina Maniscalco, Co-founder and CEO of Algorithmiq and a Professor of Computing and Logic at the University of Helsinki, was at the conference to give the keynote speech *Bringing quantum to life* and panel discussion *Accelerating medical breakthroughs through deep tech*.

She was also interviewed by CGTN Europe (owned by China Media Group), giving her opinion on the quantum global race between the US and China.

"Maybe in fifteen years from now we will have error-corrected quantum computers, Maniscalco began, "with applications using the most famous algorithms that have been discovered. For example, for cryptography, finance, logistics, so a lot is going on."

Maniscalco believes a lot remains to be seen, but they promise, she noted, that they will be disruptive and change technologies in a fundamental and big way.

She was then asked whether these technologies would create a global sensation and race to the top.

Fuelling The Growth

"I'm sure about it. And I think the competition between the different countries, including China, the US and many countries worldwide is actually fuelling the growth of the ecosystem," said Maniscalco. "I'm sure that very soon there will be clear applications that have industrial relevance."

Underlining that they will be disruptive and devoid of incremental change, Algorithmiq's CEO expressed her view that it's going to be a change in the way we live, clear and simple.

21.Post-Quantum And Pre-Quantum Security Issues Grow

by Marie C. Baca

https://semiengineering.com/post-quantum-and-pre-quantum-security-issues-grow/

General-purpose quantum computers will be able to crack the codes that protect much of the world's information, and while these machines don't exist yet, security experts say governments and businesses are starting to prepare for encryption in a post-quantum world. The task is made all the more challenging because no one knows exactly how future quantum machines will work, or even which materials will be used.

Unlike traditional computers, in a quantum computer the unit of information is a quantum bit or qubit. Qubits can have a value of 0, 1, or a superposition of both values at the same time. A broadly useful computer will need qubits that are more reliable, error-corrected, longer-lasting, and more numerous than what can be produced today.

Once developed, the power of these machines could be harnessed to accelerate discoveries in fields like AI and pharmaceuticals, not to mention security. The mainstreaming of quantum cryptography is expected to usher in a new age of data security as experts explore quantum key distribution (QKD) and other methods of cryptography based on quantum mechanics.

The flip side of this is certain encryption methods based on classical computing principles will be obsolete in a post-quantum world. That, in turn, will leave countless systems vulnerable to attacks.

But the concerns are more immediate, as well. Experts are preparing for "harvest now, decrypt later" attacks. As the name suggests, HNDL threats involve hackers collecting encrypted data now with the assumption that further developments in quantum computing will allow them to decrypt that information in the future. A recent Deloitte poll found that half of professionals at organizations considering quantum computing benefits believe their organizations are at risk of such attacks.

The solution to securing existing cryptographic algorithms is straightforward, but problematic.

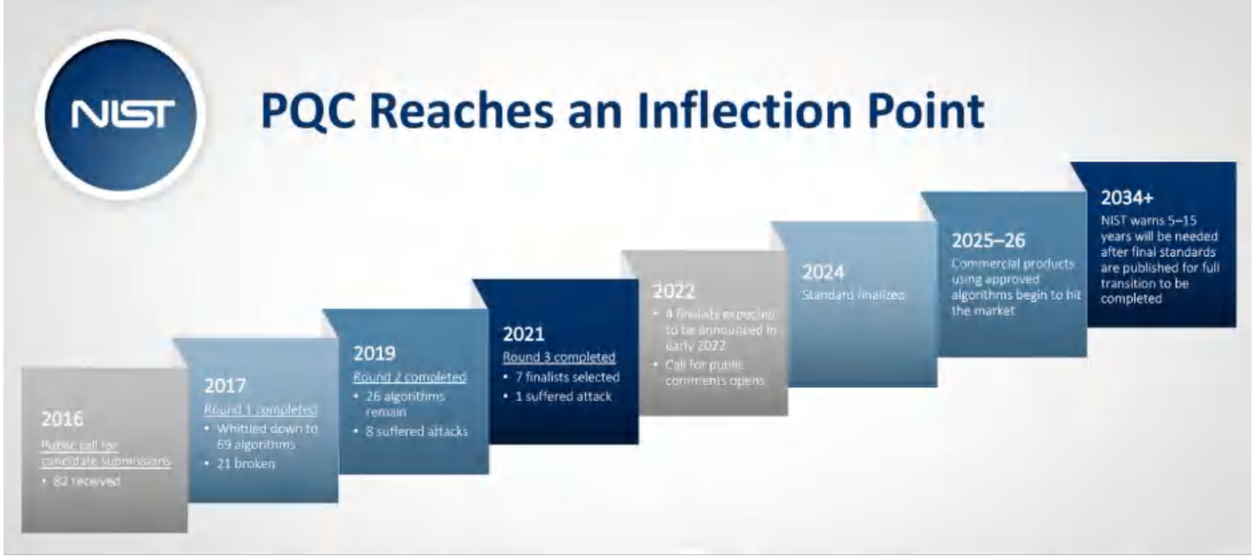
"All we need to do is replace those algorithms with newer versions that are quantum-resistant," said

Marc Witteman, CEO of Riscure. “Unfortunately, that is easier said than done.”

The extent of the challenge is illustrated by recent developments at the National Institute of Standards and Technology. In 2016, NIST asked the public for help creating and identifying cryptography standards that can withstand quantum threats. In July, NIST announced four winning algorithms and four algorithms under consideration. Then at the end of the month, researchers said they were able to break one of the four algorithms under consideration — variously called Supersingular isogeny Diffie–Hellman key exchange, SIDH, or SIKE — using only a laptop.

Witteman says SIKE’s failure is actually a good thing because it proves the necessity of NIST’s rigorous review and testing process, and shows that researchers are doing their jobs by trying to crack codes under consideration. “The design, implementation, validation, and adoption of new cryptographic algorithms is a slow and painful process.”

As the Advanced Encryption Standard was being pushed out for adoption, it took five years to replace the Data Encryption Standard in the early 2000s, but another decade for industry to adopt the new standard. This is because proving algorithmic security is hard or sometimes impossible, and updating all the relevant applications and protocols takes a massive amount of time. “Both hurdles are more painful in hardware than in software, since fixing vulnerabilities and functional updates in hardware typically requires replacement of the device,” Witteman said.



PQC Reaches an Inflection Point

2016
Public call for candidate submissions
- 82 received

2017
Round 1 completed
- Whittled down to 69 algorithms
- 21 broken

2019
Round 2 completed
- 26 algorithms remain
- 8 suffered attacks

2021
Round 3 completed
- 7 finalists selected
- 1 suffered attack

2022
- 4 finalists expected to be announced in early 2022
- Call for public comments opens

2024
Standard finalized

2025–26
Commercial products using approved algorithms begin to hit the market

2034+
NIST warns 5–15 years will be needed after final standards are published for full transition to be completed

Fig 1: NIST plans to finalize post-quantum crytopgraphy standards in 2024, but it could take between five and 15 years after that for the industry to fully adopt those standards. Source: NIST.

Dana Neustadter, senior product marketing manager for security IP at Synopsys, said quantum computing will be a particular threat to the public key infrastructure, which currently protects a wide swath of sensitive information across the internet and elsewhere, because quantum computers can be used to crack elliptical-curve cryptography (ECC), and Rivest–Shamir–Adleman (RSA) cryptosystems — algorithms that are technically solvable but would require an impractical amount of time to do so with classical computing methods.

“Hence, manufacturers of devices and systems with longer life cycles, or targeting more sensitive applications, must start implementing a path toward quantum-safe systems,” Neustadter said. “While the standardization effort is still ongoing, there is a large spectrum of candidate algorithms, some of which may be broken before or after being standardized, and knowing that a migration to a post quantum safe world will be much more complex than transitions witnessed in the past.”

However, there are paths forward. “First, symmetric cryptographic algorithms can be quantum-safe by using large keys, and hash algorithms by using larger output sizes. With regard to public keys, traditional and post-quantum cryptography algorithms will have to coexist for a while. Crypto agility in protocols and implementations will be required to be able to replace/update algorithms more seamlessly. Agility in software via firmware updates is much easier than agility in hardware. However, just like today’s algorithms, hardware acceleration and hardware implementations are required for post-quantum cryptography to meet the performance and security targets.”

Concurrently, George Wall, director of product marketing for Tensilica Xtensa processor IP at Cadence, said it is imperative for SoC designers to think about quantum security at the hardware architecture level. “By the time devices being designed today are ready for the market, it may no longer be sufficient to rely mostly on software techniques for securing sensitive algorithms or data,” he said. “There are companies focused on adopting quantum-based techniques for encryption, such as using the unique characteristics of a single silicon device to generate a unique and unclonable signature.”

Beyond cryptography

The concept of security in the quantum era also goes beyond cryptography.

Michael Osborne, CTO of IBM Quantum Safe, said during a recent webinar, “We understand quantum-safe as being safe in the quantum era. Part of that is replacing the cryptography that we use. The other part is making sure that unencrypted data becomes encrypted, or that we apply things like ‘zero trust’ to quantum. When we talk about the cryptography side, then it’s really about understanding where cryptography is being used and where it is not safe as we enter the quantum era. It’s really a more holistic perspective that we have in terms of being safe in the coming era.”

Adoption of the new algorithms does bring a risk, but waiting longer also increases risk. “Organizations that consider this change should carefully weigh the importance of keeping data confidential for a longer time to justify a transition right now,” Riscure’s Witteman said.

Those that choose to do so will find themselves in an enviable position compared with other organizations that do not see the advent of quantum computing on the horizon.

According to many experts, useful quantum computers are likely still about a decade away, but such predictions are difficult to make.

“Many companies have ambitious roadmaps that they’ve either shared publicly and intentionally, or unintentionally because they’re going public and have to release something to investors,” Eric Holland, director of strategic growth initiatives at Keysight, said in a recent presentation. “As a listener, you’re trying to figure out if they’ve improved the quality, the quantity, or the speed. If you aren’t seeing progress on those, then that implies that the device they have probably isn’t more powerful or a big step forward.”

Still, as recently as six years ago Holland encountered investors and end users who were convinced not only that quantum computing wasn’t on the horizon, but that it was actually a scam. “Those skeptics have been quelled.”

Conclusion

Like most other disruptive technologies, quantum computing has the potential to both fundamentally alter the world for the better, as well as for the worse. These powerful computers could vastly accelerate the pace of scientific innovation, but they also will render some previously sufficient encryption methods useless. HNDL attacks allow malicious parties to harvest sensitive data now and decrypt it later after the quantum computing field develops further.

Many experts agree the solution is to develop quantum-safe encryption methods, but that can be a slow and painful process. The failure of SIKE, one of the post-quantum encryption standards under consideration by NIST, proved both the difficulty of creating such standards and the necessity of doing so through a rigorous process. There are activities organizations can complete now to begin quantum-proofing their data, such as using large keys on symmetric cryptographic algorithms and larger output sizes on hash algorithms. Cryptographic agility in protocols and implementation also will be useful, and hardware acceleration and hardware implementation will be crucial. There are non-cryptographic steps to take, as well, such as encrypting unencrypted data and applying zero trust methods to quantum.

22.PQShield And Riscure Collaborate On Post-Quantum Cryptography SCA Validation

https://www.prnewswire.com/news-releases/pqshield-and-riscure-collaborate-on-post-quantum-cryptography-sca-validation-301664989.html

Riscure, a global security advisory lab and market leader in Side Channel Analysis (SCA), has partnered with PQShield, a cybersecurity company specializing in post-quantum cryptography, to evaluate PQShield's SCA testing and validation processes.

The quantum threat is high on the global security agenda, with governments and their partners planning their transition to quantum-resistance via post-quantum cryptography (PQC). In July, the US National Institute of Standards and Technology (NIST) announced draft standards for post-quantum cryptography – an important and long-awaited information security milestone.

Even when PQC algorithms are mathematically secure, they can potentially be broken by a class of exploits known as side channel attacks. These attacks exploit the PQC algorithm implementation in hardware or software rather than the underlying mathematical problem itself, and underline how important it is that any side-channel vulnerabilities are identified and addressed before solutions are widely rolled out.

PQShield is a market leader in quantum-ready cryptographic solutions for hardware, software and communications. The company is a major contributor to the NIST post-quantum standardisation project, and the draft standards it announced in July this year are all schemes contributed to by PQShield's researchers and advisory board.

Riscure provides evaluation and validation services to reinforce the security of products and components including hardware cryptographic engines, large SoCs, boot ROM, security-enhanced software applications and trusted execution environments. Riscure also provides Security Tools and Training to help companies improve the security knowledge and expertise of their development teams.

With this project, the two companies will evaluate PQShield's SCA testing process. They will also share knowledge about post-quantum cryptography and its impact on side channel attacks, advancing companies' and governments' understanding of how new quantum-secure algorithms can be secured through robust validation and countermeasures.

23.South Korea's Quantum Roadmap Presented At Ibm Kqc Hub Busan Open House

by James Dargan
https://thequantuminsider.com/2022/11/02/south-koreas-quantum-roadmap-presented-at-ibm-kqc-hub-busan-open-house/?utm_source=newsletter&utm_medium=email&utm_term=2022-11-26&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+ColdQuanta+s+Serious+Series+B+Quantum+Is+Online+in+Finland+And+More+Quantum+News

APAC Quantum

In the western hemisphere, North America and EMEA are strongholds for quantum innovation. In the Asia-Pacific region (APAC), the obvious choice is China; yet Japan, Singapore, Australia, and South Korea are doing some serious research as well.

South Korea is an interesting one, with several programs on quantum research at the university level, as well as a few startups like EYL and Qunova Computing trying to develop the technology for the commercial market, according to TQI's Quantum Intelligence platform.

Expanding on this, Kion Kim — a Researcher Director at Korea Quantum Computing Corp (KQC) — spoke at the IBM KQC Hub Busan Open House on its Roadmap.

KQC

Based in Busan, KQC is the first commercial Quantum Computing solution provider working with IBM Quantum research. KQC's main focus is on performing practical research projects, building the QC ecosystem and providing access to QC. KQC will be a leading company in KQC industry ensuring the quantum-readiness of the major companies in South Korea in near future.

"From market research, we realize that we [South Korea] are some steps behind those top-tier countries in the quantum computing world," said Kim to open his presentation.

The fact confirmed, Kim stated it was time to take action to move forward.

Kim then quoted TQI: "According to The Quantum Insider, they have more than 600 quantum computing companies in their database as of 2022…"

The Busan-based researcher then talked about the general ecosystem, again using TQI high-quality data as a benchmark, going into some detail about the hardware, software and end-user ecosystem before focusing on South Korea.

"Quantum Wave"

“They [South Korea] have a vision of moving from digital to quantum era,” Kim began. “Part of the strategy is they will train 1000 quantum experts by 2030. I think this is a very good start to build a human pipeline to create a sustainable quantum ecosystem, but it’s not sufficient, though.”

Kim is aware that building the ecosystem from the ground up is an important first step in gaining an advantage in the region and said KQC will play an important role in what he calls the “quantum wave,” with education, research and business the three key pillars of that success.

Government Actions

South Korea’s Vice Minister for Science, Technology and Innovation, Joo Young-Chang, however, recently said Korea lacked an industrial ecosystem in the quantum computing sector, which widens its technological gap with the other advanced economies,” according to an excellent article by Jin-Won Kim in *The Korea Economic Daily*.

In April 2021, the South Korean government introduced its investment strategy for quantum technology research and development, allocating 49 billion won ($37.6 million) toward its R&D budget. Whether that’s enough remains to be seen.

It looks like Busan could become what Waterloo is to Canada, an exciting quantum hub where the technology of tomorrow will be developed.

We will have to see. But whatever the outcome, South Korea will be competing with the rest in the region at some point.

24. France Transmits Its First Post-Quantum Cryptographic Diplomatic Message

https://www.diplomatie.gouv.fr/en/the-ministry-and-its-network/news/2022/article/france-transmits-its-first-post-quantum-cryptographic-diplomatic-message-1-dec

The French Embassy in the United States sent to Paris its first encrypted diplomatic message thanks to a new generation of so-called post-quantum cryptography, with the aim of withstanding the decryption capabilities of quantum computers.

Quantum computers will soon be able to crack the cryptographic algorithms used today: it is therefore essential to develop and master encryption technologies which allow us to protect sensitive communications in the future.

The message sent today, 30 November 2022, transmitted the memorandum signed on the same day between Mme Sylvie Retailleau, Minister of Higher Education and Research, and Dr Arati Prabhakar, Director of the United States’ Office of Science and Technology Policy (OSTP), aimed at supporting quantum cooperation projects between France and its American partner. The memorandum is part of the Quantum Plan announced by President Emmanuel Macron in January 2021. It follows the conclusions of the G7 in Munich of 28 June 2022, which encourage G7 nations to cooperate on strategic issues concerning the development of the quantum industry and post-quantum cryptography solutions.

For this test, carried out during President Emmanuel Macron’s State visit to the United States, the French Ministry for Europe and Foreign Affairs drew on the work of the startup CryptoNext Security, a business which emerged from research by INRIA, the CNRS and Sorbonne University and which is developing post-quantum cryptography solutions.

The French Quantum Plan benefits from €1.8 billion from France 2030. It includes a €150-million component for devising cryptographic methods resistant to quantum computing.

In the face of this systemic threat, the initiative prefigures the development of critical digital infrastructure in France. Taking into account this technological context and the current international environment, the French Government will set out an initial action plan by the end of the first quarter of 2023, incorporating a methodology and a timetable for this critical infrastructure's migration to post-quantum cryptography.

The action plan's aim will be to organize the migration to post-quantum cryptography. It will also make it possible to assert France's progress in the area, taking into account the key issues of security, technology and industrial expertise. To encourage this industrial momentum, the plan will also have to be part of a coherent European action.

25.Quantum Entanglement Will Make Quantum Internet "Unhackable" Thanks To Quantum Steering

by Alfonso Maruccia

https://www.techspot.com/news/96819-quantum-entanglement-make-quantum-internet-unhackable-thanks-quantum.html

Professor Mehul Malik has been studying quantum technologies for 15 years. With his team at Heriot-Watt's Institute of Photonic and Quantum Sciences, Malik has conceived a new way to send quantum information on optical fibers – a way that helps avoid data loss and brings the concept of quantum internet one step closer to reality.

The quantum internet is a theoretical model for a next-generation network based on the weird phenomena belonging to the quantum computing theory. The weirdest phenomenon is known as quantum entanglement, as it describes two particles or groups of particles (e.g., two photons of light) which remain connected no matter the distance. The quantum state of an entangled particle cannot be described independently of the state of the other one, regardless of the speed of light.

Quantum technology tries to harness the quantum proprieties of sub-atomic particles to develop incredibly powerful computers, or to greatly improve security for network communications and navigation systems. The problem with quantum entanglement, however, is that "transmitting" entangled photons over optical fibers becomes difficult over long distances because of noise and loss of information.

"Even the best optical fibers in the world will have a certain amount of loss per kilometer," Malik said, "so this is a big hurdle in making this form of quantum communication possible." The new research he developed with his team, however, shows for the first time that "quantum entanglement can tolerate both noise and loss – and still survive in a strong form known as quantum steering."

Quantum steering is a technique that can improve the robustness of entanglement by using "qudits," which essentially are arrays of qubits (the bit equivalent in quantum computing) arranged in multiple dimensions. The researchers used the spatial structure of light to entangle photons in a 53-dimensional space made up of "pixel" of lights.

The result: quantum steering let them transmit the entangled photons through loss and noise conditions equivalent to 79km of fiber optic cables – even with 36% of white noise like the one that could come from sunlight leaking into the experiment. Another counterintuitive finding of the new research, Malik said, was that increasing the number of dimensions in quantum entanglement also dramatically reduces the time it takes to measure the results.

"The efficient and trusted flow of information lies at the heart of modern society today," the professor explained; to build such a 'quantum' internet, "we need to be able to send quantum entanglement across real-world distances" by tolerating noise and loss in the transmission.

26.It's Time For India To Adopt Quantum-Safe Cryptography

by Amith Singhee and L.V. Subramaniam

https://www.techcircle.in/2022/11/01/quantum-safe-cryptography-is-here-it-s-time-for-india-to-adopt-it

Quantum computers are maturing quickly — perhaps even faster than we could have predicted just five years ago. We see quantum technology's rapid pace of development as an important opportunity: We believe these machines are going to solve important problems in research and industry, which could revolutionize fields from materials and drug discovery, to finance and machine learning. But this rapid development also brings about an important consideration: The encryption schemes we use today to safeguard sensitive data — such as our financial and health records — could be made obsolete in a world where future quantum computers reach their full potential.

As we work to bring about quantum-centric supercomputing, we'll need to ensure that each facet of the computing workflow can protect future systems and data from the 'harvest-now, hack-later' that's already happening. This is especially critical for governments, and highly regulated industries such as financial services, healthcare and telco. In fact, anyone responsible for securing data or digital infrastructure will need to take steps today to make themselves quantum safe. Waiting is just not an option.

Why quantum-safe matters

According to IBM's 2022 Cost of a Data Breach Report, 83% of organisations worldwide have experienced more than one data breach in their lifetime,. According to the same report, organizations in India on average reported 29,500 breaches (between March 2021-March 2022). Organizations in India, including both government and private institutions that hold sensitive data, need to immediately start implementing quantum-safe protocols.

Governments across the world are concerned that bad actors are positioning themselves to take advantage of next-generation code-breaking tools. Attackers could be stealing and hoarding large tranches of encrypted data, unreadable with contemporary tools, with the intent to decrypt it once better quantum technology becomes available. Organizations may have already experienced breaches that they will not know about for many years, creating an uncertain security and liability environment. We may not know exactly when it will be possible to breach today's encryption, but one thing is clear: any data that falls into the wrong hands before an organisation transitions to quantum-safe protocols should be considered already lost.

Setting the standards

Organisations cannot afford to wait and it is already possible to start using secure cryptography. In July 2022, the U.S. Government's Department of Commerce's National Institute of Standards and Technology (NIST) announced four quantum-safe protocols as their "post-quantum cryptographic standards," which they expect to finalize in the next couple years.

While securing critical Indian data with quantum-safe cryptography will be important, there is also a huge opportunity here for Indian engineers and the IT industry. India's IT industry received its biggest boost when the Y2K problem happened at the turn of the millennium. Companies around the world scrambled to fix the date change problem that could have potentially cripple industries, ranging from finance and airlines to mining on January 1, 2000. In many cases it required going through thousands and millions of lines of code to fix the bug. This needed trained programmers. And the Indian software industry seized the opportunity.

Fixing the "YQK" problem — this time, the "Q" stands for "quantum," — presents an even bigger opportunity for India. This is the time for decisive action from the Indian standards organisations, industry and government, to both address the challenge and to figure out ways in which the Indian IT industry can contribute and take advantage.

Don't wait

With so-called 'quantum advantage' on the horizon, business leaders should be preparing for how their industry could benefit. But they should also understand the risk of future fault-tolerant quantum computers on the horizon, and explore available solutions based on quantum-safe cryptography standards, such as the IBM hybrid cloud system z16, that will protect their data and classical systems.

In conclusion, any computer system that will have to operate securely without major modifications over a period of years — the computer in your next car, or embedded in a satellite, for example — will need to be quantum secure well in advance of the threat. Can you afford to wait?