Crypto News

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

November 01, 2022

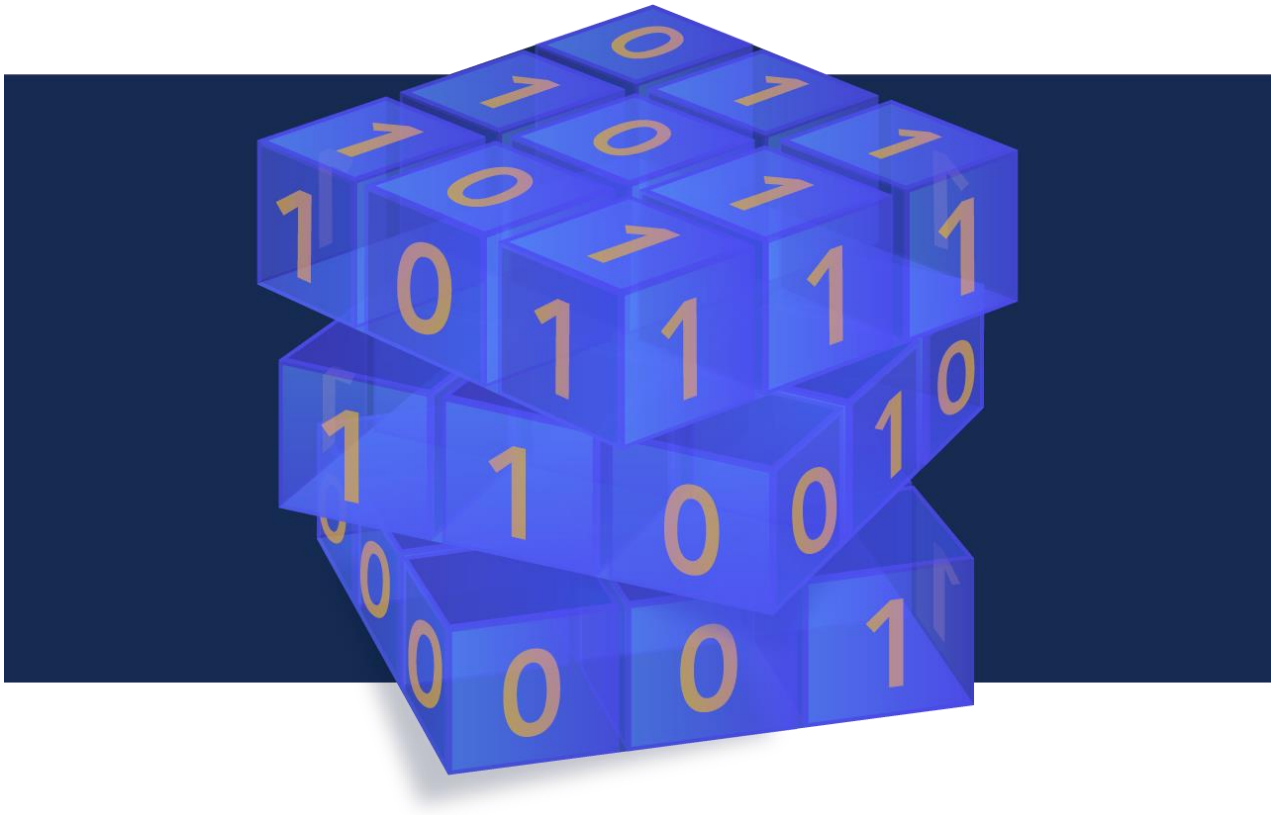

TABLE OF CONTENTS

Editorial

Welcome to another edition of Crypto News! This month we have a number of fantastic articles for you to peruse. Let's start at the end of the newsletter this month and work our way to the beginning. Take a look at article 22 which gives insight into Cloudflare's post-quantum cryptography support for websites and APIs that are served through their network. This is approximately a fifth of the internet. Don't forget to note the reference to Countdown to Y2Q which is a term coined by our humble working group to represent April 14, 2030 as the date when we estimate quantum advantage to be showcased by quantum computers. Next, take a few minutes to read article 16. It gives an overview of how quantum computing will affect cybersecurity and truly revolutionize it. It also highlights the companies that are taking pro-active strides to prepare for a post-quantum world by fortifying their cybersecurity solutions to address the threats that quantum computing poses. Last but not least, head over the article 7 which indicates that some nations may choose to adopt different PQC Standards from the US. This is a decision that they will make independently but it may result in a disruption in their ability "to interact seamlessly with the rest of the world" if they work outside of ISO or IETF. As always, there are many other interesting articles for you to choose from so go ahead and dive in!

The Crypto News editorial is authored by Mehak Kalsi 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.Toppan and NICT Establish World's First Technology for Equipping Smart Card Systems with Post-Quantum Cryptography Selected by NIST

https://whattheythink.com/news/112768-toppan-nict-establish-worlds-first-technology-equipping-smart-card-systems-post-quantum-cryptography-selected-nist/

Toppan, a global leader in communication, security, packaging, décor materials, and electronics solutions, and the National Institute of Information and Communications Technology (NICT) have developed PQC CARD®, the world's first smart card equipped with post-quantum cryptography, which is difficult for even a quantum computer to crack. The organizations have also successfully confirmed effectiveness by applying PQC CARD® to control access to H-LINCOS, a system for the secure long-term storage and exchange of healthcare data.

PQC CARD® uses CRYSTALS-Dilithium, a next-generation digital signature algorithm selected as a potential standard technology by the U.S. National Institute of Standards and Technology (NIST) in July this year. PQC CARD® was developed in collaboration with ISARA Corporation, a company with cutting-edge post-quantum cryptography technologies.

Toppan and the NICT will take advantage of this technology to advance development of quantum secure cloud technology5 that enables the secure communication, storage, and use of highly sensitive information. Going beyond smart card security, the two organizations will also target the establishment of safe and secure social infrastructure based on the creation of fundamental technologies that ensure security for day-to-day internet-based activities, including email, online shopping, cashless transactions, and online banking.

Part of the research was supported by two Japanese government programs: the Cabinet Office's Cross-ministerial Strategic Innovation Promotion Program (SIP) "Photonics and Quantum Technology for Society 5.0" and the Ministry of Internal Affairs and Communications' Research and Development for Construction of a Global Quantum Cryptography Network (JPJ008957).

2.ISARA makes four digital certificate patents publicly available to boost quantum security

https://www.helpnetsecurity.com/2022/10/26/isara-digital-certificate-patents-quantum-security/

ISARA revealed that it is dedicating the intellectual property behind its ISARA Catalyst Agile Digital Certificate Methodology — including four patents — to the public.

Industry leaders, including Crypto4A, DigiCert, Entrust, ISARA, Keyfactor, PKI Solutions, Sectigo, and Venafi, are among those who promote secure, crypto-agile solutions to ease the quantum computing migration path for organizations.

Hybrid certificates, an important component of ISARA's Catalyst methodology, enable organizations to have a seamless, cost-effective, and simplified migration to quantum-safe security today to protect connected devices and the Internet of Things (IoT) — as well as complex public key infrastructures (PKIs) —

with no impact to end users. These certificates support two or more cryptographic algorithms within a single certificate and can support both classic and quantum-safe public keys and signatures.

A hybrid certificate is a traditional X.509 digital certificate that has additional quantum-safe components encoded within it. One of the key characteristics of hybrid certificates is the ability to simultaneously support existing systems as well as those that have been upgraded to be quantum safe. When an organization starts to migrate its systems and applications to quantum-safe cryptography, they won't need to support two separate PKIs — one for traditional certificates and one for quantum-safe certificates — since they will already have two-in-one hybrid certificates in place. This provides backward compatibility during the transition period to quantum.

Most of the cryptographic products, protocols, and services that businesses rely on every day need to be upgraded to become quantum safe. This requires an agile migration strategy that preserves compatibility with existing systems so that organizations can prioritize migrating their most critical systems first without negatively impacting the systems to be upgraded later.

Industry-wide support for crypto agility and crypto-agile certificates

"At ISARA, we believe an industry-wide, crypto-agile ecosystem is important to make it easier for organizations to implement quantum-safe solutions now and to help with the quantum migration," said Atsushi Yamada, CEO at ISARA. "By making these four critical digital certificate patents available to the public, we are looking to grow the industry and increase crypto-agile implementation for more secure systems now and in the future."

"As we enter the quantum age, we face the daunting task of migrating our existing and future systems to become quantum safe. Hybrid certificates provide a powerful, agile, and elegant methodology that greatly enhances our migration capabilities. I would like to thank ISARA on behalf of the cybersecurity community for dedicating this important technology to the public as together we ensure continued trust of our digital systems," said Bruno Couillard, Co-Founder, CEO and CTO, Crypto4A.

"Crypto agility will be essential for surviving the transition to post-quantum algorithms. To ensure digital trust is maintained, the industry needs to work together and ISARA's decision to remove a potential obstacle to rapid deployment of hybrid certificates is greatly appreciated. ISARA's leadership will increase the accessibility of crypto agility and help companies prepare for a post-quantum world. DigiCert is proud to be working with ISARA to help companies and their users have confidence that their online interactions, transactions, and business processes are secure," said Dr. Avesta Hojjati, VP of Research and Development, DigiCert.

"The timeline for post-quantum computing development is unclear, but once a quantum computer is able to break RSA and elliptic curve cryptography, the transition will be abrupt, and organizations need to start preparing now. As such, we're delighted that ISARA has chosen to gift this methodology to the public," said Greg Wetmore, VP Product Development at Entrust. "The industrial applications of public key cryptography are wide and diverse. The migration to post-quantum cryptography will need a set of tools equally diverse in order to meet a range of security and agility needs. We are pleased that Catalyst Hybrid Certificates will join the publicly available toolbox along with multiple certificates, and composite approaches to help organizations prepare for the transition to a post-quantum world."

"The potential threat of quantum computers to computer security and secure communications is potentially the biggest existential threat our industry has faced to date. It's on us to help ensure that the transition from conventional to post-quantum cryptography is as smooth as possible and hybrid certificates are a key part of that," said Tomas Gustavsson, Chief PKI Officer, Keyfactor.

"The crucial importance of future-proofing identity and data encryption cannot be overstated," said Mark B. Cooper, President & Founder, PKI Solutions. "Every single day, we address risks and misconfigurations in this industry. This hybrid methodology from ISARA is part of the much-needed evolution to a new secure cryptographic environment for organizations around the world."

David Mahdi, Chief Strategy Officer, Sectigo, CISO Advisor and former Gartner Analyst commented, “We welcome this news from ISARA Corp. and concur that open standards and interoperability must be built at the heart of the modern cybersecurity tech stack. While the much touted ‘Quantum Apocalypse’ may seem like a distant problem to solve, governments and organizations of all sizes must begin preparing for the inevitability that our current cryptographic standards become obsolete. The ubiquity of cryptography in computer systems, including critical infrastructure cannot be ignored and so enabling organizations of all sizes to start their journeys to quantum readiness is vital to maintain the digital trust we all rely on now and in the future.”

“Venafi created the Machine Identity Management market and we’ve been consistently investing in innovation and open-source technology for years,” said Kevin Bocek, VP of Strategy and Threat Intelligence for Venafi. “Venafi sponsored both Crypto4A and ISARA to further the innovations that were important to enabling this open-source technology and we’re excited to see it become open to all. Our goal is to make it easy to be ready for the post-quantum world where today’s machine identities can’t be trusted.”

Crypto-agile patents dedicated to the public:

- US9660978
- US9794249
- WO2018027300
- JP6644894

3.MASTERCARD’S NEW CARD: SAFER FROM QUANTUM ATTACKS?

by Lewin Day
https://hackaday.com/2022/10/25/mastercards-new-card-safer-from-quantum-attacks/#more-559636

Quantum computers present a unique threat to many aspects of modern information technology. In particular, many cryptographic systems could be at risk of compromise in the event a malicious actor came into possession of a capable quantum computer.

Mastercard is intending to stay ahead of the game in this regard. It has launched a new contactless credit card that it says is impervious to certain types of quantum attack.

HACK-PROOF?

The card is based on new industry standards from EMVco, a technical body that works in the secure payment space. Known as the EMV Contactless Kernel Specifications, they outline functionality for payment devices like ATMs and point-of-sale terminals to process transactions. The specification includes a new “Secure Channel” method of communication between card and reader that aims to protect against common attacks like eavesdropping, relay, and man-in-the-middle attacks. The new cards are intended to be compatible with existing payment hardware out in the field.

The main highlight of the new cards, though, is in how they operate, cryptographically speaking. Traditionally, payment card systems have relied on public-key cryptography, using methods like the ever-popular RSA algorithm. As explained in our public key encryption primer, the theory is simple. A private key is two prime numbers, and the public key is their product. Encrypt a message using the public key, and it can only be decrypted with the prime numbers in the private key. The problem for attackers is that even though they know the public key, it’s very difficult to figure out the private key, simply because finding two large prime factors of an even larger number is hard.

That is, unless you have the help of a quantum computer. A quantum computer with a sufficient number of qubits can run Shor's algorithm to quickly find prime factors of very large numbers. This can be used to reveal the private key for a wide variety of encryption algorithms. This would crack open everything from world financial systems to the encrypted documents of governments and companies around the globe. The one benefit we currently have is that no quantum computer with enough entangled qubits yet exists to break our commonly-used algorithms. Experts believe it's only a matter of time, however, and even the US government is rapidly moving to alternative quantum-secure encryption methods.

Mastercard's new plastic will thus shift towards new algorithms it says are "quantum-resistant," and thus not subject to these attacks. This will also involve the use of longer key lengths to further increase the robustness of the encryption method. Ease of use is also important, though, so the new system will keep the authentication process to under 0.5 seconds.

Interestingly, the documentation from EMVco indicates that the new cards will include Elliptic Curve Cryptography (ECC) for authentication purposes. Traditional ECC is not actually considered quantum-secure. In fact, for the key lengths currently in common use, ECC is likely slightly easier to break than RSA with a quantum computer.

So it could just be marketing bluster from Mastercard. It would seem foolhardy for one of the world's largest payment processors to roll out new technology that was already known to be incapable of solving the stated problem. Instead, it's perhaps more likely that Mastercard is using some new variant of ECC that is potentially secure against typical quantum computing attacks. Various ideas have sprouted in this area, though some have recently been proven insecure. Maybe they are focusing on some other algorithm, but will also support ECC. But then how to stop degrade attacks?

Overall, it's a good thing that companies like Mastercard are already pursuing quantum security. Rolling out such infrastructure takes plenty of time, after all. Plus, once a quantum computer is up and running in the hands of a malicious actor, it will be far too late to act. However, at the same time, new encryption methods must be rigorously explored to ensure they indeed deliver on the security we need them to have. Here's hoping the new cards have been subject to such due diligence.

4.Quantum Benchmarking is Important Yet is Still in Its Infancy

by Yuval Boger
https://quantumcomputingreport.com/quantum-benchmarking-is-important-yet-is-still-in-its-infancy/

Performance benchmarks provide users with a frame of reference to compare products in the same category. Many popular classical benchmarking tools exist, such as MLPerf for machine learning, PassMark, and 3DMark for GPUs. It stands to reason that quantum computing users can benefit from similar tools.

Benchmarks are critical as users struggle to translate hardware characteristics such as gate fidelity, coherence times, and qubit connectivity into meaningful business insight. After all, as enjoyable as the underlying technology might be, business users want to know how soon they can get valuable results from a given computer or, more generally, which computer (if any) is best to solve a particular problem. Benchmarks are also helpful to validate claims from vendors, such as claims about gate fidelity or the efficacy of error correction, and serve as internal development tools for such vendors.

Indeed, several commercial, academic, and standards organizations have launched benchmarking, such as those from IBM, QED-C, Super.tech, The Unitary Fund, Sandia National Labs, and Atos.

These benchmarking suites typically fall into two categories: 1) system performance tests that measure hardware-related parameters such as speed and noise, and 2) application performance tests that compares

simulated results of reference algorithms to actual execution results on various hardware platforms.

In my opinion, one type of benchmark that's missing is a way to determine the best hardware to execute a bespoke algorithm or program that an organization has developed. Some might call this "predictive benchmarking," which might also consider the known or measured imperfections of a particular platform to predict and recommend the best one for a given application. Such predictive benchmarking is interesting for two reasons: 1) there could be dramatic variance in execution quality between different quantum computers, and 2) because organizations have access to multiple types of machines through quantum cloud providers, it would not be difficult to switch platforms if the results warrant it.

Recently, I had the opportunity to discuss benchmarking with Pranav Gokhale, VP of Quantum Software of ColdQuanta (and formerly CEO of Super.tech, acquired by ColdQuanta). Gokhale and his coworkers started working on benchmarking in the middle of 2021 and published their suite of open-source benchmarks, called SupermarQ as well as comparative measurements earlier this year. SupermarQ includes application-centric tests in domains such as logistics, finance, chemistry, and encryption, while also including a test measuring error correction performance. Pranav mentioned that a key design goal of their suite was to allow it to scale to a large number of qubits while maintaining a seemingly conflicting goal of classic verifiability.

I asked Pranav about market feedback on their product. He mentioned significant commercial and academic interest in benchmarking various algorithms and devices and interest from hardware vendors that leverage SupermarQ to track progress in their hardware development. Interestingly, Pranav reports that SupermarQ results often diverge significantly from predicted results that rely solely on qubit coherence and gate fidelity numbers. He says this happens because imperfections are often correlated (such as qubit crosstalk). As such, Super.tech believes their benchmark suite helps de-hype the quantum market, demonstrating real-world performance metrics for quantum computers.

Many hardware vendors could have legitimate claims about the inaccuracy of benchmarking suites. Vendors might claim they can rewrite and optimize these test applications for their platforms by using platform-specific features, native gates, or a better configuration of their transpiler. As several recent hackathons and coding competitions have shown, there are numerous ways to implement any given algorithm, sometimes differing in orders of magnitude in their efficiency.

In classical machine learning, Alexnet, the winner in a global competition to develop an image classification algorithm, revolutionized the field. Suppose quantum computing organizations initiated similar efforts, providing sample data sets and seeking the best quantum solution. In that case, vendors could demonstrate the power of their quantum platforms with optimal algorithms and settings. Both end-users and researchers might benefit from such efforts.

Benchmarking is important. Without it, we'd be comparing the proverbial apples to oranges. But quantum benchmarking still appears to be in its infancy.

5.What to Look Out For as the IT Community Starts Implementing PQC

https://quantumcomputingreport.com/what-to-look-out-for-as-the-it-community-starts-implementing-pqc/

It's been a little over three months since NIST announced the first Post Quantum Cryptography (PQC) algorithms selected after Round 3 for standardization and additional ones undergoing further study in Round 4. Since then there have been other developments including an announcement that one of the Round 4 candidates, SIKE, has been broken and also a call by NIST for proposals for additional PQC digital signature algorithms in order to provide more diversity. In addition, NIST kicked off a Migration to Post-

Quantum Cryptography Project and recruited a a consortium of twelve corporate partners to bring awareness of the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms.

To get a better feel for how the implementation is going and an idea of some of the key issues we interviewed a few individuals involved in the PQC efforts to get their views on selected topics. Individuals we talked to include Thomas Pöppelmann from Infineon, Vincent Berk from Quantum Xchange, Rebecca Krauthamer from QuSecure, Vadim Lyubashevsky from IBM, Wil Oxford from Anametric, Michele Mosca and Andrew Hammond from evolutionQ, and Jack Hidary from SandboxAQ. We learned several interesting things.

The first question we asked was when do they recommend a CIO get serious about starting a quantum safe program within their company. **The universal answer we received from the experts is that an organization should start one immediately, if they haven't already done so.** They also saw challenges in convincing some users of the need for immediacy. CIO's already have multiple non-quantum related cybersecurity problems and are certainly not eager to add an additional one. Also, the quantum threat is not as readily visible as something like a ransomware attack. There is no hard deadline on when becoming quantum safe is absolutely needed, which was a huge motivating factor with Y2K. And within a corporation, cybersecurity is viewed as a cost center rather than a revenue generator. So getting a budget for this from corporate management is a little more challenging. In a few cases, there is some naivety from end users about how hard it is to implement post quantum security. Some may believe it is just another firmware update that they will be able to quickly implement. Although that may be true for consumer devices like PCs and cell phones, for enterprise computing and IoT devices, it will be much more complicated.

An additional challenge with CIOs who do follow PQC and the NIST competition is the recent breaking of the Rainbow and SIKE algorithms. They are also aware that although NIST has selected some algorithms, the formal approval and publishing of the standards with recommended parameters is still about two years off. So, some of them are worried about implementing a technology which is not fully baked! The CIOs don't want to spend a bunch of money to implement a PQC algorithm in their organization and find out later that it gets broken.

The PQC vendors, of course, have multiple arguments against these concerns. First, they point out that converting to a quantum safe infrastructure will take a long time. It is not as simple as implementing a simple firmware update. To start, identifying all the areas where a PQC upgrade is needed can be a challenge. Many enterprise CIOs have IT infrastructures have been created over a multiple decades and many of the original implementers may no longer be working at the company. Just taking an inventory of where cryptography is used in the infrastructure may be a challenge. One of the tools PQC vendors can deploy to help this are the various analyzers that can inspect a network and identify where cryptography is used. Jack Hidary of SandboxAQ mentioned that this was a benefit they derived from their acquisition of Cryptosense. Although both companies had analyzer software of their own, the two pieces were complementary, and SandboxAQ has already integrated the two pieces together to have something even more effective.

Another recommendation we heard from many of the vendors is to use hybrid algorithms that combine the classical RSA or Elliptical curve encryption with one of the PQC algorithms. There are several reasons for recommending this approach. First, it provides some insurance in case a weakness is found in the PQC algorithm. A hacker would not only have to break the PQC algorithm, but also the classical RSA or elliptical curve algorithms too. And the classical algorithms have already survived for several decades without anyone finding a weakness. In addition, end users are very reluctant to have vendors work on routines deep within their systems, particularly with software modules involved with security. It is much easier for an end user to accept a vendor adding additional modules outside their core infrastructure than to do a rip and replace of a module deep inside their systems. In fact, some companies in regulated industries may have requirements to continue using the classical cryptography due to certain standards they need to meet. And, it is expected that these standards will be very slow to change.

One concept we hear frequently is that of crypto agility. The overall architecture of the PQC modules should be implemented so that it is easy to change parameters or complete algorithms. As mentioned above, there

are still concerns that a weakness might be found in the future in a selected algorithm or a recommend is made to change the specific parameters used with a particular algorithm. The NIST competition was designed with this possibility in mind because it has emphasized selecting multiple algorithms that can be used for achieving algorithm diversity. Although it takes more effort to design an agile architecture that can more easily adopt to different algorithms than a design to fit a very specific one, it may well be worth the effort. One area where agility may be more of a challenge is to design IoT chips with integrated cryptography modules. These devices are typically more constrained in memory, processor performance, power, and cost than larger computers that are installed in a data center. So the chip companies will need to work hard to provide agility in a single chip.

One trend we heard from several of the vendors was to recommend the use of quantum random number generators (QRNG) as the entropy source for creating the encryption keys. Today, most classical encryption systems uses pseudo-random number generators and the concern was that with the increased power of large computers and the use of advanced machine learning, there is a possible risk of someone discovering the key. In addition, the PQC algorithms generally require larger key sizes and many more key exchanges in order to complete a communication. So more entropy is required and using non-deterministic QRNGs helps to reduce the risk. evolutionQ has published a good report titled *Quantum Random-Number Generators Practical Considerations and Use Cases* for more information.

Another consideration for implementing PQC is the need for testing. A user should remember that converting from classical encryption to one of the PQC or hybrid approaches will likely result in changes in the system latency, key sizes, and ciphertext size. Although in many systems, this may not matter, there may be a few systems where is causes a problem. So this is another reason why it is wise to start now to provide time for testing to be performed and fixes implemented before an enterprise goes live.

Nonetheless, the vendors are reporting increased level of interest from end customers investigating PQC. Converting the worldwide digital communications infrastructure to utilize quantum safe approaches will take 10-20 years and require massively more resources than any previous security upgrade. The vendors are reporting that some of the earliest adopters are within the DoD, banks, and telecom companies. Although the PQC algorithms are open sourced that will be significant revenue opportunities for vendors in this market by providing ancillary software and consulting services. And the vendors are taking different approaches to serving their customers. Quantum Xchange has developed a product called Phio Trusted Xchange (TX) that provides a unique key delivery system and crypto-diverse management platform and eliminates single points of failure. QuSecure has just signed a distribution deal with Arrow Electronics to have Arrow's 8,000-person sales force represent QuSecure's solution to its federal and commercial customer base. SandboxAQ has taken an unusual approach for a startup company and has established a Strategic Investment Program to invest in or acquire other companies working in this segment. And IBM has announced a new z16 mainframe computer with built-in functionality to provide quantum-safe cryptography.

So there will be many opportunities for the vendors of quantum safe products in the years ahead and we just hope they can stay one step ahead of the bad guys who will do everything they can to break into systems using any security hole they can find.

6.Global Encryption Day: Cyber-securing your data with quantum-safe cryptography and confidential computing

by Alessandro Curioni

https://www.weforum.org/agenda/2022/10/global-encryption-day-cyber-securing-your-data-with-quantum-safe-cryptography-and-confidential-computing/

Cyberattacks are on the rise, with cybercriminals getting ever smarter. But so are security researchers, always striving to be a step ahead of the most sophisticated hacker – to keep you, your data and your business safe.

With companies more and more under pressure from data protection regulations and the risk of fines if data is not properly protected, researchers are coming up with innovative ways to enhance data privacy.

October is Cybersecurity Awareness Month in Europe and the US, a month to remind us to be aware of the constantly evolving cyber threats and be prepared for them. With the latest milestones in artificial intelligence (AI) and cryptography, security researchers are pushing the limits of cyber defences.

They are on the front line of fighting cybercrime, along with the first incident responders – and must keep adapting to threats that spill more and more into our physical world from the digital one.

Today's tech giants, among them IBM, are harnessing the power of AI to protect businesses, organizations and individuals against cyber criminals – even those that may want to use future quantum computers to crack modern encryption. That's where quantum-safe cryptography comes in.

The rise of quantum computing

While even the ancient Greeks, Romans and Egyptians used symbol-replacement encryption, modern computer technology has brought cryptography to totally new heights. Data is routinely encrypted when deemed sensitive. The problem is, as cryptography keeps maturing, so is an emerging but incredibly promising type of computation – quantum computing.

First talked about in the early 1980s as a possible practical application of quantum mechanics, quantum computers are now a reality. They rely on nature's weird and wonderful properties when atoms and subatomic particles can be entangled and in multiple states simultaneously.

These properties enable quantum computers to perform many more computations than a traditional computer ever could. As they become more powerful, quantum computers soon should be able to crack modern encryption.

That's why cryptographers have recently been busy developing a type of encryption based on the mathematical property of lattices that would keep data safe from a future quantum computer.

In July, the US National Institute of Standards and Technology (NIST) announced four schemes primed to pave the way to new quantum-safe crypto standards for the world to adopt.

Move to quantum-safe cryptography

IBM's Security and Quantum research teams contributed to developing these schemes. But the journey to quantum-proof your data security doesn't stop here; it's just the beginning. Companies should be thinking about migrating their systems to quantum-safe cryptography already today.

That's also the view of the US National Security Agency. It recently announced that its networks with classified data will switch to quantum-safe standards by 2025. And it doesn't matter that quantum computers are not powerful enough to break modern encryption just yet. They will be sooner than you might think.

At this year's Mobile World Congress, the GSM Association (GSMA), a body representing the interests of mobile network operators, announced the formation of the GSMA Post-Quantum Telco Network Taskforce, with IBM and Vodafone as initial members. The taskforce aims to help define policy, regulation and operator business processes to better protect telecoms from future quantum computers.

There are already offerings with quantum-safe encryption, such as IBM's recently released z16 and Linux-ONE Emperor 4 systems that protect against software and physical attacks. And we are not stopping there.

The recently-chosen standards cover only encryption and authentication, but all signs indicate that we will need much more advanced cryptography in the near future. With users and companies becoming more sensitive to protecting private data, bleeding-edge technologies like distributed ledgers and zero-knowledge proofs are being pushed into the real world.

The most efficient protocols underpinning the privacy of these constructs is currently not quantum-safe, and we are in the process of developing ones that are efficient and will remain secure in the quantum future.

The cyber secure realm of confidential computing

Moving to quantum-safe standards will take the world a few years at least. And this will not be enough to make your sensitive data safe today, especially in the cloud. Enter confidential computing.

This technology aims to ensure that your data in rented cloud infrastructure stays encrypted not only in storage or in transit but also when it's in active use – during, say, training machine learning models, indexing the data, or manipulating it in some other way.

Confidential computing isolates data within a protected central processing unit (CPU), ensuring the confidentiality of a workload thanks to hardware mechanisms giving protection to entire virtual machines (VMs), often called 'secure' VMs, and containers.

These secure virtual computer systems sport their own CPU, memory, storage and network interface, giving customers access to their own 'computers' in the cloud rather than through dedicated physical hardware.

A secure virtual machine is akin to a highly protected hotel room. Only the customer can use their key to enter the room, while the hotel staff can't. Similarly, a secure virtual machine protects a user's workload from the cloud provider's personnel and software, and from other (potentially malicious) clients that may be running on the same infrastructure.

Recent years have seen huge leaps in confidential computing, with many tech giants betting on it, including Intel, Google, ARM, Microsoft and others. IBM Z, widely used in the financial industry, is a secure, reliable and scalable platform for confidential computing.

While confidential computing protects a program from external attacks, preventing an adversary from directly accessing information inside it, we've also recently developed 'memory-safety protection' to defend systems from internal threats.

Currently still a research project, this technology protects a program from internal attacks. It's aimed at preventing an adversary from exploiting memory safety vulnerabilities within a program to steal information, as was the case in the HeartBleed attack, or from taking control of a program, as happened in Return Oriented Programming attacks.

Fully homomorphic encryption is the Holy Grail

While confidential computing relies on dedicated hardware and the robustness of the software stack running in the secure enclave to keep your data safe, researchers are also pursuing what's known as fully homomorphic encryption (FHE).

Traditional encryption schemes secure data at rest and in transit but require it to be decrypted before any computations occur. However, with FHE, one can achieve complete end-to-end data security and privacy, with data never being decrypted at all.

This way, the technology provides cryptographical security at the data level regardless of the underlying infrastructure or environment where the processing is performed. It means that with fully homomorphic encryption, one can safely outsource computations to the cloud or to a third party, and even have multiple parties share and gain insights from data – all while preserving privacy.

Researchers have been tinkering with this mathematical concept since the 1970s. A major breakthrough came in 2009 when Craig Gentry, back then an IBMer, published his seminal work – *A Fully Homomorphic Encryption Scheme*. His paper provided the mathematical underpinning for the emergence of technologies enabling complex industry workloads to be run over encrypted data.

While the promise of FHE was transformational until recently, the computational overhead and the complexity of usage made it not very practical for the industry to apply. But researchers keep pushing the limits to develop more efficient, fully homomorphic encryption schemes – and we are getting there.

Cybersecurity researchers always a step ahead

At IBM, we now offer a downloadable package, free for non-commercial use, to experiment and develop applications and machine learning models over encrypted data.

We are also busy working on a cloud-native infrastructure to give customers access to different services over encrypted data, with an initial focus on serving machine learning models.

Cyber criminals may be getting more sophisticated – but cybersecurity researchers will always be a step ahead.

7.China, Russia to Adopt ‘Slightly Different’ PQC Standards From US

by Nancy Liu
https://www.sdxcentral.com/articles/analysis/china-russia-to-adopt-slightly-different-pqc-standards-from-us/2022/10/

Quantum computing experts expect China and Russia to select encryption algorithms for post-quantum cryptography (PQC) standards based on the same mathematical problems as the U.S. and other western countries, while choosing a scheme that is slightly different.

The constant threat that quantum computing poses on classic cryptography is a global problem, Michael Osborne, CTO of IBM Quantum Safe noted during a recent virtual roundtable. Based on his observations, “the algorithms that [will be] standardized in China or in Russia or in wherever that they have been based on the same mathematical problems that quantum computers threaten.”

NXP cryptography researcher Joppe Bos said he expects other countries’ PQC selection will mirror what they did for classical cryptography. This model is that they defined different elliptic curves rather than the one standardized by the National Institute of Standards and Technology (NIST), whose primary focus is the U.S. government. “That is just a sign that they wanted to have something for themselves, and it's all based on the same heart mathematical problem,” Bos said.

Bos expects China to standardize PQC algorithms that are based on “very, very similar problems from exactly the same families” that are being considered for standardization by NIST.

“[Such as] lattice-based crypto or hash-based schemes, these are exactly the schemes these countries are

looking at as well," he added. "That gives a lot of confidence, fortunately, in the security of the schemes, but they might choose a scheme which is just slightly different or with different parameters."

Lattice-based PQC is built on a family of math problems called structured lattices and Dustin Moody, post-quantum cryptography project lead at NIST, identified it as the best family that was being evaluated during the institution's selection process. The institution also selected algorithms that use hash functions as a backup to avoid relying only on the security of lattices for signatures, NIST noted.

"An observation with China is actually they selected derivatives of at least two of the algorithms that were also selected. by NIST as their standard for cryptography in China. So essentially, they're aligning with the protection that we're also aligning with," Osborne said. "It means they're also cognizant of the threat and also comfortable with the technology selections, or the mathematical problems that we're comfortable with."

The Chinese Association for Cryptologic Research (CACR) held a post-quantum cryptography competition and announced its results in early 2020. The top winners were lattice-based Aigi-sig, LAC.PKE, and Aigis-enc. The last one is based on the asymmetrical learning with errors (LWE) problem.

PQC Standardization Progress: US vs. China

NIST initiated its post-quantum cryptography competition in 2016, announced the first group of winners in July of this year, and aimed to publish its PQC standard by 2024.

Meanwhile, CACR sent out a notice for its competition in 2018, and named the winners in 2020. China reportedly plans to start the PQC standardization process around this year and expects to begin the commercial migration around 2025.

"China's certainly spending a lot of money they're investing a lot to develop their quantum technologies to build a quantum computer or to do other very interesting applications with quantum technologies. So the U.S. is definitely aware of that. China's certainly doing all they can to advance the state of the art for their own purposes. And that's another reason we need to have this quantum-resistant cryptography in place to protect against that," Moody said during the virtual roundtable.

Will Non-Western Countries Adopt International PQC Standards?

Laura Thomas, former CIA case officer and current chief of staff and VP of strategic initiatives at ColdQuanta, told SDxCentral that non-western countries are more likely to follow international standards set by the International Organization for Standardization (ISO) or the Internet Engineering Task Force (IETF).

"And if they do develop the standards outside of ISO or IETF, they're not going to be able to interact seamlessly with the rest of the world, and that will have to be a consideration that they make," Thomas said.

On the other hand, NIST works with those international institutions. "To a large degree, these other standards organizations were very happy with what we were doing at NIST and wanted to wait for our process to finish before they selected algorithms themselves," NIST's Moody said in an earlier interview, adding he expects NIST's selections will be adopted by the international standards institutions and they likely will add other algorithms from other countries.

8.Post-Quantum Cryptography: Anticipating Threats and Preparing the Future

by ENISA

https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future

The new report published by the European Union Agency for Cybersecurity (ENISA) explores the necessity to design new cryptographic protocols and integrate post-quantum systems into existing protocols.

Can we integrate post-quantum algorithms to existing protocols? Can new protocols be designed around post-quantum systems? What's the role of double encryption and double signatures? What changes will new post-quantum algorithms impose to existing protocols? These are some of the questions the report published today intends to answer.

The transition to post-quantum cryptography (PQC) does not end with the selection and standardisation of post-quantum algorithms. Integration with existing systems and protocols is also required. The report focuses on the necessity to resort to future-proofing and for the acquisition of knowledge not limited to external standards.

The report expands on the initial aspects of those post-quantum cryptography challenges addressed in the study published last year by ENISA: Post-Quantum Cryptography: Current state and quantum mitigation.

Why do we need to anticipate the rise of quantum technology?

Scientists commonly agree that quantum computers will be able to break widely used public-key cryptographic schemes, when they come into being. Because, in reality, systems using this new technology do not widely exist yet.

The transition to new quantum resistant cryptographic algorithms is expected to take years due to the complex processes and financial costs. This is why we still need to anticipate this and be prepared to deal with all possible consequences.

The report answers the difficult questions raised by post-quantum cryptography in order to make sure we will avoid jeopardising today's public key cryptosystems, e-commerce, digital signatures, electronic identities, etc. This will be critical, even if rolling out new cryptographic systems might prove impossible for a number of systems with restricted accessibility such as satellites.

If quantum technology is sought after, it is because it can provide efficient solutions to the technical challenges we face today. Unfortunately though, this new technology also comes along with novel threats to the security of our equipment and systems because quantum computing will make most currently used cryptographic solutions insecure and will end up changing the existing threat models radically. We will therefore need to quickly adapt before this happens to avoid threats that might compromise our infrastructures.

So what can we do today?

The report includes a number of technical recommendations such as:

- Developing guidelines for major use cases to assess the different trade-offs and systems best matching application scenarios;
- New protocols or major changes in existing protocols should be PQC aware, taking into account the integration needs of PQC systems;
- The use of a hybrid systems which could translate into a post-quantum cryptography added as an extra layer to pre-quantum cryptography.

9.Securing India’s cyberspace from quantum

techniques

by Arjun Gargeyas and Sameer Patil
https://indianexpress.com/article/opinion/columns/securing-indias-cyberspace-must-take-steps-to-tackle-newest-threat-8212744/

Last month, there were reports that the Indian Army is developing cryptographic techniques to make its networks resistant to attacks by systems with quantum capabilities. The Army has collaborated with industry and academia to build secure communications and cryptography applications. This step builds on last year's initiative to establish a quantum computing laboratory at the military engineering institute in Mhow, Madhya Pradesh.

With traditional encryption models at risk and increasing military applications of quantum technology, the deployment of "quantum-resistant" systems has become the need of the hour. This requires upgrading current encryption standards that can be broken by quantum cryptography. Current protocols like the RSA will quickly become outdated. This means that quantum cyberattacks can potentially breach any hardened target, opening a significant vulnerability for existing digital infrastructure. Hack proofing these systems will require considerable investments.

This is a challenge that India will have to proactively deal with as cyber risks arising from quantum computing are accentuated by the lead taken by some nations in this sector. For example, the US National Quantum Initiative Act has already allocated $1.2 billion for research in defence-related quantum technology. Particularly worrying for India is the fact that China now hosts two of the world's fastest quantum computers.

India is getting there slowly but steadily. In February 2022, a joint team of the Defence Research and Development Organisation and IIT-Delhi successfully demonstrated a QKD link between two cities in UP — Prayagraj and Vindhyachal — located 100 kilometres apart.

China's quantum advances expand the spectre of quantum cyberattacks against India's digital infrastructure, which already faces a barrage of attacks from Chinese state-sponsored hackers. India's dependence on foreign, particularly Chinese hardware, is an additional vulnerability. The question then arises: How to make India's cyberspace resilient?

In 2019, the Centre declared quantum technology a "mission of national importance". The Union Budget 2020-21 had proposed to spend Rs 8,000 crore on the newly launched National Mission on Quantum Technologies and Applications. This has to be complemented by a strong focus on securing cyberspace from quantum attacks.

Currently, India has very few capabilities in developing advanced systems capable of withstanding quantum cyberattacks. India must consider procuring the United States National Security Agency's (NSA) Suite B Cryptography Quantum-Resistant Suite as its official encryption mechanism. The NSA is developing new algorithms for their cypher suite that are resistant to quantum cyberattacks. This can then facilitate India's official transition to quantum-resistant algorithms.

The Indian defence establishment can consider emulating the cryptographic standards set by the US's National Institute of Standards and Technology (NIST) which has developed a series of encryption tools to handle quantum computer attacks. It has developed a series of four algorithms to frame a post-quantum cryptographic standard. After adopting these technical steps, India must start its national initiatives to develop quantum-resistant systems. For this, the government can fund and encourage existing open-source projects related to post-quantum cryptography along with active participation in the Open Quantum Safe project — a global initiative started in 2016 for prototyping and integrating quantum-resistant cryptographic algorithms.

Two, the country should start implementing and developing capabilities in quantum-resistant communications, specifically for critical strategic sectors. QKDs over long distances, especially connecting military outposts for sensitive communications, can be prioritised to ensure secure communications whilst protecting key intelligence from potential quantum cyberattacks. Eventually, this can help establish a nationwide communication network integrated with quantum cryptographic systems, thereby protecting cyberspace from any cross-border quantum cyber offensive.

Finally, diplomatic partnerships with other "techno-democracies" — countries with top technology sectors, advanced economies, and a commitment to liberal democracy — can help India pool resources and mitigate emerging quantum cyber threats. The world is moving towards an era in which the applications of quantum physics in strategic domains will soon become a reality, increasing cybersecurity risks. India needs a holistic approach to tackle these challenges. At the heart of this approach should be the focus on post-quantum cybersecurity.

10.Dutch influence standards for post-quantum cryptography

by Kim Loohuis
https://www.computerweekly.com/news/252526051/Dutch-influence-standards-for-post-quantum-cryptography

The US National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools designed to withstand the attack of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on today.

Léo Ducas, senior researcher in the cryptology group at the Netherlands' Centrum Wiskunde & Informatica (CWI), the national research institute for mathematics and computer science, is involved in the two most important algorithms of the upcoming NIST portfolio – one for public key encryption and one for digital signatures.

According to Ducas, who is also a professor at the University of Leiden, these new standards are inevitable because there is nervousness about the arrival of quantum computing. "We know quantum computing will not be rife tomorrow, but this standardisation procedure and its deployment take time," he said. "Obviously there is certain sensitive information that needs to be secure and confidential – not just at present, but in the future as well. Take state secrets, for instance."

Cyber security experts have warned that hackers are stealing data now to decrypt it in the future, when quantum computing could render modern encryption methods obsolete. A report published by NIST in April 2016 cited experts that acknowledged the possibility of quantum technology rendering the commonly used RSA algorithm insecure by 2030. "We need to be ready for that," said Ducas. "This means we have to anticipate now."

The announcement of the chosen tools follows a six-year effort managed by NIST, which started in 2016 with a call for the world's cryptographers to devise and then vet encryption methods that could resist an attack from a future quantum computer. A total of 23 signature schemes and 59 encryption schemes were submitted, of which 69 were deemed complete and proper. The NIST competition consists of four rounds, during which some schemes are discarded and others studied more closely.

In July this year, NIST announced the first group of winners from its competition, which included Crystals-Kyber and Crystals-Dilithium, both developed by an international collaboration in which CWI participated. Other team members are ENS Lyon, Radboud University, Ruhr University Bochum, University of Waterloo, IBM, NXP, ARM, SRI International, Florida Atlantic University and Tsinghua University.

“It was a rather big team, but that was the key aspect,” said Ducas. “It consisted of both industrial and academic people, and all their knowledge was necessary to develop the algorithms we have. Take NXP, for example – they build chips and already use cryptology to embed in those chips. We needed their knowledge for the design, because it is essential that what we develop not only fits into devices like smartphones and laptops, but also in other places where chips are being used, like in the automotive industry. Fitting cryptology can be a big challenge.”

Apart from the two algorithms in which CWI was involved, two further algorithms for signatures were selected by NIST – Falcon and Sphincs+. Sphincs+ also was partially conceived in the Netherlands, led by Andreas Hüsling from TU Eindhoven.

Ducas added: “The selection of our schemes as a standard means that it will be deployed globally, protecting the privacy of billions of users. Fundamental research rarely gets such a direct and broad impact. The credit should go to the whole cryptographic research community. Whe schemes we proposed are merely the crystallisation of decades of scientific effort.”

The algorithms developed by the international team are based on lattices, one of Ducas’ specialities. “Both were designed together and share more than just the same mathematical platform,” he said. “We tried to make them look alike, so they will be easy to implement together.” The Falcon algorithm designed for signatures also uses a lattice platform.

“But that is where the similarity ends,” said Ducas. “This algorithm has different advantages and drawbacks.”

One of his biggest concerns is that this algorithm computes with floating point numbers, as opposed to integers. “Computers are obviously equipped to do this, but it is a real challenge for cryptology”, said Ducas. “Rounding can differ from computer to computer, so it has challenges for implementation. But because of its shorter keys, it was also selected for the NIST portfolio.”

Now the four algorithms have been selected, they need to be written down into proper standards. “This is obviously where NIST comes in, whereas we are mainly academics and technicians,” said Ducas. “NIST will draft up the ultimate text for the standard, but it will be in coordination with us.”

NIST hopes to publish the standardisation documents by 2024 but, according to Wikipedia, may speed up the process if there are major breakthroughs in quantum computing.

After the release of the standards, the industry needs to be pushed to put them to use, said Ducas. “I have a suspicion that most companies will want to be post-quantum resistant, so I think these standards will be easier to push than, for example, the hash function update from SHA-1 to SHA-2,” he said. “Moreover, I think IBM and NXP will incorporate their own designs within their own products.

“Eventually, NIST is pushing the core of the new standard, the mathematical knowledge, but on top of that, there are a lot of things that are involved, like protocols, documentation, and so on. It might even evolve into an ISO standard, who knows, but NIST is leading the crowd.”

So, will the new standards ensure we will be safe from quantum computers’ ability to possibly crack the RSA encryption? “This is related to the P versus NP problem,” said Ducas. “The best guarantee we can have are the years of documented failures. This is the case with existing cryptology, and still is the case with post-quantum cryptology.

“There is reasonable confidence to deploy, but no absolute mathematical guarantee. This is why we often say that cryptographers seldom sleep at night.”

11.A Detailed Guide on Quantum Cryptography with Pros and Cons

by Eden Allen
https://hackernoon.com/a-detailed-guide-on-quantum-cryptography-with-pros-and-cons

Quantum cryptography is the next level of encryption used today. Originating from principles of physics, this segment of encryption involves the mechanisms of physics mixed with computing power. This computing power and quantum mechanisms are used to create two powerful security systems, quantum key distribution, and quantum-safe cryptography.

We will take you through the details of quantum encryption and cryptography in this guide. Going forward, you will also learn about how quantum cryptography works and what its applications are in our world.

Explaining Quantum Cryptography

Quantum Cryptography applies the tenets of quantum mechanics to encryption and cryptography. With the mechanisms of quantum integrated into encryption, the resultant security is so tightened that no one can access the data being shared and secured with this system.

Even if a hacker would have access to quantum computers and the entire kit, they cannot crack the encryption provided here. This is because quantum encryption leverages quantum's multiple states and the "no change theory" to secure the information.

There is no doubt that quantum encryption is better, more reliable, and more authentic than the traditional cryptographic measures we are using till today. The highly popular Advanced Encryption Standard (AES) makes the data virtually unhackable, but it does not make anything impossible to hack.

Alice and Bob Demonstration

To depict the working behind quantum encryption, we were given a case example that will help make things more clear. So, take that Alice wants to send a message to Bob. As she writes the message and runs it through the polarizer to polarize every single photon to change its orientation into a particular type. This can be horizontal, vertical, or diagonal.

The encryption key here is the change in the orientation of the photons. Upon receiving, Bob would guess the polarizer and decode the message. Here Bob would guess and match the photon cases with the ones Alice has generated.

In this case, suppose there is another person who is trying to access the message. In the crypto world, this person is called Eve. Eve is using its own polarizer for accessing the message. In case Eve uses the polarizer for decoding purposes, Bob and Alice would say that there are discrepancies because we cannot change the property of a photon without moving or changing it.

With this principle at the backend, quantum cryptography was developed and used as a protective measure to secure data, transactions, communication, and information.

Principles Behind Quantum Cryptography

Quantum cryptography leverages individual particles of light like photons for data transmission and transfer. This data is transmitted over fiber optic wires. The photons represent binary bits, hence the security depends on the execution of quantum mechanics.

The utilization of photons or light particles is effective because these particles can exist in two or more places simultaneously. Also, any quantum property cannot be changed or observed without first changing it, and the particles cannot be copied.

With these aspects, quantum cryptography is able to provide the highest form of security. Some might say that the keys shared via quantum cryptography are unhackable because of the principles of photons applied here.

However, we are seeing some possibilities of getting around the security provided by this system. But nothing has been proved or demonstrated as of yet and even with quantum computing power, hacking a quantum key is not easy.

Let's get into some detail about photons. Every photon passed through the encryption system in quantum cryptography represents a binary code number. It can be either 0 or 1.

The key represents a string of 1's and 0's creating a coherent message that only the two entities involved can use for encryption and decryption. The way quantum computing encryption works is similar to the AES, but due to the properties of photons, we can see a big change in security.

The binary bits converted from the photons provide a distinct spin to the photons. It can be vertical (|), horizontal (-), diagonal to the right (/), or diagonal to the left (\). This provides a unique code or cryptographic property to the key.

Heisenberg's Uncertainty Principle

This principle states that we cannot measure or calculate the position and momentum of an object. This principle does not apply to the macroscopic world because minute changes in that world are often ignored.

But in a quantum world, even the slightest change can make a big difference. Hence, the Heisenberg Uncertainty Principle has a big role to play in quantum computing and cryptography.

Why is there a Need for Quantum Cryptography?

Have you heard of the phrase, "Necessity is the mother of invention"? Well, the inception of quantum encryption and cryptography has a similar story. With the coming of quantum computing, the existing encryption standards may have become vulnerable.

Using Shor's algorithm in quantum computing, computers have broken the asymmetric encryption. Normal computers cannot find the prime number that is the key to finding the decryption key in the RSA encryption standard. But a quantum computer can find the prime number. Hence it can break the key.

For the AES, the AES-128 bit and AES-256 bit have become vulnerable with the brute force attack from a quantum computer. While they are still not hacked, the brute force attack has reduced the security net.

This is to the extent that the AES-128 bit is reduced to AES-64 bit, and the AES-256 bit is reduced to AES-128 bit. The AES 128-bit standard is still strong enough to protect the information, but we can say that it is only a matter of time before quantum computers can crack the code.

Quantum-Safe Cryptography and Quantum Key Distribution (QKD)

Two concepts come out of quantum encryption and cryptography;

Quantum-Safe Cryptography

Quantum-Safe cryptography identifies the methods, efforts, and algorithms that will make a key resistant to attacks. It basically identifies the measures that will make any piece of data secure from hacking attacks from a classical computer we use in daily life or a quantum computer.

The focus here is on quantum computers because they have higher computing power and possibilities.

Quantum-Safe cryptography is also called Post-Quantum cryptography. At present, NIST is working to solicit, evaluate, and standardize quantum-resistant public key cryptographic algorithms. Once they are approved and standardized, quantum cryptographic keys will become available for public use.

The existing encryption standards like AES, ECC, RSA, etc., use mathematical equations to generate cipher text. But with quantum cryptography, we can generate cipher text with physics and mathematical equations, both.

Quantum Key Distribution

Quantum Key Distribution (QKD) involves sending data in the form of photons across an optical link. The motive here is to ensure the protection and security of the data, and QKD provides it easily because of the systems generated with quantum cryptography.

The higher form of security provided by QKD stems from the fact that it can easily detect any sort of intrusion. This will alert the interested parties or entities, and the key used for data transmission can be discarded.

QKD is most commonly used in communications channels. We can select from a number of protocols to implement QKD. But it requires a quantum channel and an authenticated classical channel.

The quantum channel sends the state of light in the form of photons and the classical channel is for the sender and the recipient.

Is Quantum Safe Cryptography “Unhackable”?

In every discussion about quantum encryption and cryptography, the laws of quantum mechanics will always pop up. The activity where encryption keys are sent in the form of photons to and fro between two entities is theoretically untraceable.

The fiber optic lines are the key element in this system. We have discussed all the fiber optic lines and how they make transmissions secure. However, there is another way of transmission used here, where satellites are used to exchange the keys.

In the satellite-based approach, the principle of Entanglement comes into play. China has been using this technology for sending and receiving quantum-safe cryptography data and messages.

Digressing a little from the topic here, in entanglement, two particles are entangled to a level that they achieve the same state. Once this is achieved, one of the particles is sent to someone else. After the particle is received at the other end, it is ensured to have a similar state as its twin.

In case, one of the particles changes, the other particle will change to match is not an assured fact. This is because we are not using the entanglement for communication purposes.

So, we cannot use this property for communication, but it can be used to share encryption keys, which then can be used for securing communication over traditional channels.

Based on the equipment, technology, and systems applicable in this system, we can say that, at present, quantum cryptography is unhackable. Yes, even with the quantum computing systems we have access to today, hacking communication, data, and transmission is not virtually possible.

Benefits and Disadvantages of Quantum Cryptography

Given its advantages, quantum encryption and cryptography also have a few disadvantages. Let's go through the benefits first.

Benefits of Quantum Encryption

- **Communication is Secured:** With quantum cryptography, the communication is secured to a higher level than a traditional encryption standard. Since it's based on the laws of quantum physics, communication is more secure.
- **Multiple Security Methods:** Quantum computing and physics help provide the required security via different methods. We have discussed entanglement and polarizer in the sections above. But more methods can be derived in the future with more research and development.
- **Detecting Eavesdropping:** With quantum-safe cryptography, we can detect if any party other than the two entities authorized to access the data is trying to trespass.

Limitations of Quantum Cryptography

Even a technology as good as quantum cryptography has its limitations.

1. **Limited by Range**: Since the entanglement system has limited applications, we have to rely on fiber optical cables to implement quantum encryption. And these wires can only be laid for a limited distance. The longest we have is up to 500 KMs.
2. **Polarization Changes**: Photons are susceptible to changing their polarization, even when they are in transit. This can lead to higher error rates.
3. **Costly Equipment:** Not just the fiber optic cables, but all kind of equipment required to setup and install a quantum cryptography system is highly expensive.

Conclusion

From mathematical equations helping us secure our data and online communication to using physics for the same purpose, we have evolved. With quantum computing and cryptography allowing businesses, governments, and organizations to secure their data further, it is going to become virtually impossible for hackers to hack into systems and eavesdrop into conversations.

Even with its limitations, quantum encryption and cryptography are highly secure and useful. Once approved for public use, we can expect its limitations, especially about the higher costs going down once it gets more traction.

In the time to come, we can see a large-scale implementation of cryptographic technology.

12.IBM Leader Explains 'Downstream Impact' of Quantum Computing

by Tommy Clift
https://www.sdxcentral.com/articles/interview/ibm-leader-explains-downstream-impact-of-quantum-computing/2022/10/

GSMA announced a Post-Quantum Telco Network Task-force last week at MWC Las Vegas to develop quantum-safe cryptography standards within the telecom industry. While a fault-tolerant quantum computer is still many years away according to IBM VP and Fellow Ray Harishankar, that doesn't mean both it's possibilities and threats aren't nascent.

"When such a computer is available, what does it do to cryptography? That's the question," Harishankar told SDxCentral.

Current computers rely on bits for calculations while quantum computers harness exponential power of quantum bits (qubits) – which can compute a simultaneous mix of ones and zeros to create or solve intensely complex problems that challenge even the most powerful supercomputers today, GSMA stated in the press release about the Post-Quantum Telco Network Taskforce.

Harishankar explained that while it may be easy to discern the prime factors of 55 [11 and 5], with larger integers, this process becomes harder and extremely time consuming to calculate. "If I were to give you a number that is 637 digits now and ask you to compute that, you can't even survive enough time to figure it out," Harishankar explained. "It's going to take hundreds of years for classical computers to do that, whereas quantum computers can do that in a relatively short period of time."

"And that speed up is what concerns us," he continued. Because now, when a fault tolerant, scalable, quantum computer is available, people will be able to crack the asymmetric public key encryption mechanism."

With the sensitivity of information going increasingly digital – be it financial, medical, or otherwise – developing a preemptive safeguard is urgent. "That's why we want to create algorithms that will solve that problem both on classical and quantum, so it cannot be broken in the future."

Harishankar holds a background in physics and computer science, and while he leads the business and technical strategy for IBM Quantum Safe, he had much to offer within how quantum will propel progress across many industry standards.

"I wish I was a student today; this is fascinating stuff," he exclaimed. "The solving of the problem is one thing. But the downstream impact of that and its impact on communities is significant."

Quantum Will Spur Innovation

"The positive side of it is certainly what we accentuate. You have no idea what people are going to apply quantum for, and the potential is immense," Harishankar said.

"I think you will find in the next 20 years or so – when quantum becomes mainstream – a significant explosion in innovation. The types of problems people are able to solve and the impact that it has is going to be unbelievable."

While Shor's algorithm was the original quantum algorithm to break the encryption within public key cryptosystems, Harishankar explained "a parallel algorithm called Grover's algorithm, which is essentially doing a faster search," can be applied to revolutionize AI advancement.

"An AI model can be construed as a sparse matrix, and you have to go and search for the right information. Quantum enables you to do that much faster, right. So many of the advances that we wish to make in AI can be made possible," he explained.

Among additional use cases, Harishankar listed widespread optimization, where network, traffic, and delivery optimization will offer not just monetary benefits, but societal and environmental solutions. Additionally, all the modeling for portfolio balance and actuarial analysis within financial services stand to benefit.

Within battery technology, Harishankar said quantum will guide development for 3D visualization of molecules and elements like never done before. “That is going to be a significant breakthrough for not just biologists, but solid state mechanics and material science folks who can go look at this and create new materials,” he said, adding, “That’s where most of the work is being done in applying quantum to solve key challenges that we couldn’t solve before.”

13.Data security: post-quantum cryptography transition underway

by James Tyrrell
https://techhq.com/2022/10/post-quantum-security-solutions-making-their-way-to-market/

Qubits offer a mind-bending upgrade on the classical ones and zeros that support today’s digital world. Rather than just representing either a one or a zero, qubits can – somewhat counterintuitively – be both. In fact, qubits can point to combination of values, or parallel realities, which coverage towards the most probable outcomes. And while this is great news for using quantum computers to predict the weather, discover new pharmaceutical drugs, and explore advanced materials, there’s a wrinkle. The computing boost provided by quantum processing is expected to make light work of breaking the encryption keys currently securing data on the web. “In quantum, you can do everything at once,” Skip Sanzeri, Chief Operating Officer at **QuSecure**, told TechHQ.

Planning opportunity

The good news, in terms of keeping our data safe, is that such powerful quantum computers are unlikely to be in existence today. Scientists around the world have made tremendous progress in building qubits using superconductors, semiconducting quantum dots, trapped ions, photons and range of other technology platforms. But none of those quantum computers is thought to be sufficiently powerful to reverse engineer the various cryptosystems (most obvious as the padlock shown in your browser search bar) that users currently rely on to keep their data safe.

However, with each round of updates, quantum computers move another step closer to unravelling the hard sums that fox today’s classical machines and underpin current data security. And, in the wrong hands, quantum computers could allow attackers to read information that we’d rather they didn’t.

Sensibly, **in 2016, US national standards agency NIST launched a competition to identify quantum-resistant encryption algorithms**, and is now writing the leading prospects into security standards that are expected to be published in 2024. But that doesn’t mean that companies and organizations need to wait around until then before giving thought to what a transition from classical to post-quantum cryptography might involve. Picturing the vast scale of the modern internet, it’s clear that the number of devices and data stores affected is huge.

“It’s not rip and replace,” advises Sanzeri. “Begin with the most vulnerable sites and start your planning now.” Currently in beta, QuSecure has a product that allows customers to create quantum safe channels between end-points. And big-name partners listed on the firm’s website include Amazon, Google, and Microsoft – to give just a few examples. Focused on communications, the data security solution sits within existing protocols such as TLS. “We put a second pipe inside that’s quantum safe,” Sanzeri explains.

Cryptographic agility

At the algorithm level, QuSecure is using the NIST candidates, with software added on top to enable the post-quantum cryptography. And Sanzeri comments that solutions perform well even for hardware with limited processing power. “We have invented a way where if any device is connected to the internet, we

can create a quantum safe channel without loading up the endpoint," he said. Also, to accommodate any unforeseen issues in the strength of the NIST algorithms – which is a reasonable assumption, given the uncertainties surrounding the new world of post-quantum cryptography – the system is built to be 'crypto-agile'. Algorithms can be changed and rotated, as necessary, to preserve security and maintain the integrity of post-quantum cryptography.

Putting yourself in the shoes of an adversary and thinking about what information assets could be at the top of an attacker's wish list, you'd probably chose communications channels. The live conversations that are being had today between businesses leaders, governments and other international organisations are likely to contain the most pressing and up to date information. Pictured in this way, is straightforward to see why QuSecure, and others, are choosing to bring post-quantum cryptography solutions to this area first.

Last month, **IBM and Vodafone announced that they were joining the GSMA Post-Quantum Telco Network Taskforce**, and US telecommunications firm AT&T has reportedly commented that it intends to be 'quantum ready' by 2025. These actions add more weight to the overall consensus that a quantum computer powerful enough to decrypt the data that's being passed around today is likely to arrive sooner rather than later. Data operators that don't take these risks seriously could find themselves in dire straits. The ability to read information travelling over the internet would expose a huge amount of sensitive data, including conventional financial details, the communications between cryptocurrency wallets and exchanges, and much more.

Better safe than sorry

QuSecure estimates that 90% of encrypted web data relies on RSA-2048, which could, theoretically, be exposed using quantum computing hardware consisting of 4100 Qubits. **IBM recently updated its quantum development roadmap through to 2025** when the computing giant hopes to hit 4158+ qubits. But, unlike IBM, adversaries are unlikely to be so transparent about their quantum computing capabilities, so better to plan ahead while the opportunity allows.

In fact, many organizations may have little choice – for example, national security memorandums issued by the White House direct Federal agencies to set requirements for updating cryptographic systems. And organizations such as the World Economic Forum have issued sound **advice on how to transition to a quantum-secure economy** [PDF] and avoid the so-called risk of 'encryptogeddon', which points to a phased approach as being a useful template to follow.

14.AT&T Aims to be 'Quantum Ready 'by 2025

by Nancy Liu
https://www.sdxcentral.com/articles/news/att-aims-to-be-quantum-ready-by-2025/2022/10/

AT&T is aiming to become "quantum ready" by the year 2025, claimed a quantum security and preparedness team member during this week's AT&T Security Conference.

The tier-one operator has been identifying its cryptographic assets, vetting post-quantum cryptography solutions, and taking trials to identify those solutions, according to Brian Miles, principal member of tech staff at AT&T.

"We've got AT&T quantum ready on our roadmap by 2025," Miles said, adding that that doesn't mean the company will be fully quantum secured.

"This just means that we have done all our due diligence," he explained. "And we have a clear path forward

and we have all the solutions identified to target and address some of the different problems posed by quantum computing."

That effort should put the operator in a better position before the cryptographically relevant quantum computer (CRQC) emerges. CRQC is defined as a quantum computer that reaches the compute capability to break an RSA-2048 key using Shor's algorithm, according to Miles. Shor's algorithm is a quantum computer algorithm developed in 1994 by American mathematician Peter Shor.

The consensus of industry experts for now has identified the year 2034 as a potential target date for CRQC to emerge, he said.

AT&T: Start Building a Crypto-Agile Architecture Now

Amid the "harvest now, decrypt later" threats, more organizations started their quantum preparation journey. One of the first steps that experts recommended is to understand organizations' potential exposures.

Miles also urges organizations to implement cryptography agility, which is a framework or architecture that allows companies to replace their cryptographic primitives, underlying cryptography, and encryption algorithms with little or no impact on the existing applications.

"In a nutshell, that means you get off board your cryptography, get it out of your applications, get it more centralized, ultimately put automation in place to make the underlying infrastructure [transition] relatively painless," he explained.

The next significant step is to identify the cryptographic assets and who has the responsibility for that inventory within the company, Miles noted.

"It's incredibly important to get started on a crypto-agile architecture roadmap within your company quickly," he said. "The whole crypto-agile architecture at least gives you the tools and the ability to pivot to different cryptography on short notice."

15.Infinity extends face biometrics to cryptographic identity systems with ZeroVault launch

by Chris Burt
https://www.biometricupdate.com/202210/infinity-extends-face-biometrics-to-cryptographic-identity-systems-with-zerovault-launch

Infinity has announced that its ZeroVault engine has been extended to blockchain wallets, distributed ledgers and other cryptographic identity systems to deliver biometric account binding, authentication, and recovery.

ZeroVault is part of the ZeroFace product, which can be integrated with cryptographic systems, according to the announcement. ZeroFace is the flagship product of the ZeroBiometrics platform launched in July.

"We asked ourselves: 'What if you could log into and recover your blockchain wallet with something you can't lose or forget?'," says Alfred Chan, CEO of Infinity. "What if we could make all cryptographic identity systems as easy to use as unlocking your phone? That's exactly the experience you can create when you use the new ZeroVault feature within ZeroFace."

ZeroVault enables ZeroFace to integrate seamlessly with deployments of the BIP39 technology used for mnemonic codes that are used by cryptographic wallets as seeds to create encryption keys, Infinity says. Fast and accurate authentication or account recovery can then be performed with ZeroFace biometrics, with BIP39 recovery also available as a recovery option.

Two-factor biometric authentication can also be enabled for higher-security use cases. ZeroVault can also be implemented for more advanced applications with the individual's ZeroHash used to create transaction signing keys that the company says cannot be stolen, as they only exist while the user is authenticated.

ZeroVault can be integrated into Android and iOS applications, with features executed locally on the user's device.

The ZeroBiometrics platform was recently integrated into EclipseIR's software for security camera feeds.

16.Quantum Computing to Revolutionize Cyber Security

by Max Golderstein
https://www.investing.com/analysis/quantum-computing-to-revolutiinise-cyber-security-200630684

The cybersecurity industry has come to the spotlight this year with Russia's invasion of Ukraine. Russia is believed to have attacked Ukraine's IT infrastructure just days before invading it. In addition, Uber recently reported a major cyberattack, prompting the company to initiate a thorough investigation into the events. These are not isolated incidents. According to security and aviation giant Leonardo, the global cost of cyberattacks eclipsed $6 trillion in 2021. It includes governments, multinational companies, enterprises, SMBs, and even individuals targeted by cybercriminals. Although cybersecurity companies have developed advanced tools to fight cyber criminals, it seems as if cyber criminals themselves are using complex, highly effective technologies to carry out these attacks. This has created an urgent need for cybersecurity companies to develop better solutions to safeguard sensitive data and systems. Furthermore, quantum computing is another significant threat to cybersecurity solutions today. Still, a few companies are leading the charge in revolutionizing the cybersecurity industry by developing solutions that address these challenges while embracing quantum computing to strengthen their products.

Quantum Computing Revolutionizes Cybersecurity

Quantum computing uses the laws of quantum mechanics to solve problems deemed too complex to be solved by conventional computers. This field of science focuses on how nature works at minor scales. Although quantum computing may not be able to improve the performance of conventional computers in everything they do, the cybersecurity industry will undoubtedly benefit from using quantum computing in many ways. However, there is a downside risk, as quantum computing could be used to nullify the encryption technologies that are in use today.

First, quantum random number generation could be used to generate numbers and combinations that are truly unique, enabling cybersecurity software to strengthen the security measures deployed to any given network. Second, quantum key distribution can be used to share cryptographic keys in a way that guarantees security, as this mechanism can even alert users of the presence of an unauthorized third party. Third, large-scale quantum computers are believed to be able to crack today's encryption mechanisms, such as RSA and Diffie-Hellman. It would take advanced post-quantum cryptography to protect sensitive data from vulnerabilities arising from this possibility. The growth of quantum computing, therefore, is forcing the cybersecurity industry to rethink its technologies and data encryption mechanisms.

The cybersecurity industry will have to strike a balance between using quantum computing to strengthen

its product offering and addressing the vulnerabilities of current cybersecurity systems exposed by quantum computing. A few companies have emerged as frontrunners in doing this.

Companies to look out for

In light of the opportunities and threats presented by quantum computing, many tech companies have taken initiatives in the recent past to develop cybersecurity solutions that address the threats posed by quantum computing while using the same technologies to foolproof their product offering.

- **Microsoft** is one such tech giant at the forefront of this movement. The company, in recent quarters, has highlighted the importance of developing post-quantum cryptography to build encryption systems that cannot be deciphered easily with quantum computing. The company recently launched the NIST Post-Quantum Project, inviting cryptographers worldwide to submit candidates for peer review. Microsoft is currently experimenting with four post-quantum project candidates: FrodoKEM, SIKE, Picnic, and qTESLA. With its deep pockets, Microsoft is well-positioned to spend millions of dollars in R&D investments to build cybersecurity solutions that alleviate the threat posed by quantum computing.

- **CrowdStrike**, a cybersecurity company that protects sensitive data on cloud networks, is another company to look out for in this space. The company offers intelligent threat detection solutions and Zero Trust identity protection for its clients and is working on developing quantum-safe encryption algorithms. With many businesses moving to the cloud amid the rising popularity of hybrid work, CrowdStrike, focusing on cloud networks, is likely to emerge as a big winner in developing quantum-safe cybersecurity solutions.

- **Fortinet,** a cybersecurity company based in the United States, provides automated cybersecurity solutions that offer 360-degree protection for sensitive data and networks. The company recently decided to support Singapore's National Quantum-Safe Network project to promote security solutions that negate the threat posed by the rise of quantum computing. Fortinet is already distributing quantum-safe VPN solutions, and the company remains committed to protecting customer data using advanced technologies with low failure risk.

- **Hub Cyber Security** is another company to look out for in the cybersecurity space. The company's confidential computing solutions are some of the only "quantum-ready" solutions. HUB is already partnering with QuantLR to develop a quantum security solution for the Israeli Ministry of Defense and other high-end customers such as government entities and multinational organizations. This year, the company has agreed to merge with SPAC Mount Rainier Acquisition Corp. (RNER) and is already collaborating with private and government entities in Israel and other key markets to deploy cybersecurity solutions that address the threat quantum computing poses.

- **Zscaler**, another cloud security company that serves clients worldwide, is worth monitoring as the company's Secure Services Edge architecture is being developed to fight the risks brought on by quantum computing. The company is considered a leader in the zero-trust security space. It offers private access solutions designed to provide safe access to managed applications hosted on both the private and the public cloud.

Conclusion

The rise of quantum computing offers opportunities and challenges for the cybersecurity industry. As a result of this, the industry is changing dynamically today. Both established and young companies are developing solutions to protect sensitive data from the risks posed by quantum computing while making the most of this advanced technology. These companies are likely to gain lucrative financial rewards in the long run.

17.LG Electronics : Signs MOU to Bring Enhanced Cybersecurity to Connected Vehicles

https://www.marketscreener.com/quote/stock/LG-ELECTRONICS-INC-6491575/news/LG-Electronics-Signs-MOU-to-Bring-Enhanced-Cybersecurity-to-Connected-Vehicles-41929101/

Company to Integrate Post-Quantum Cryptography with Algorithm Optimization into Its Advanced In-vehicle Infotainment Systems.

LG Electronics (LG) has signed a memorandum of understanding (MOU) with LG Uplus, a South Korean mobile network operator, and CryptoLab, a South Korea-based cryptographic company specializing in post-quantum cryptography (PQC) technology. Under the agreement, the three parties will work together to develop PQC technology for enhanced automotive cybersecurity.

With the growing number of connected cars being made, the demand for cybersecurity solutions that can protect vehicle systems and passengers' personal information continues to rise. PQC, also known as quantum-resistant cryptography, is a new technology that is replacing the public-key cryptographic system currently used in the quantum computing environment. The technology has been widely adopted in software-focused industries, including telecommunications, data and application security services.

Working collaboratively with its fellow MOU signatories, LG plans to proactively apply PQC technology to its in-vehicle infotainment (IVI) systems, providing increased electronic security to its global automaker partners.

Through the new agreement, LG will secure a next-generation cryptographic system that will help to significantly upgrade automotive security. Ultimately, the company aims to create a more secure connected vehicle environment, encompassing key areas such as over-the-air (OTA) updates, point-of-interest (POI) services and vehicle-to-everything (V2X) services.

"In the automobile industry, the importance of cybersecurity continues to increase," said Eun Seok-hyun, president of the LG Vehicle component Solutions (VS) Company. "This is why it is critical for us to secure core digital security technologies and apply them to our hardware- and software-based solutions for vehicles. As a leader in the vehicle components market and a trusted future mobility partner, LG is committed to making connected vehicles as safe and secure as possible."

18.Nobel Prize in Physics Goes to Pioneering Quantum Entanglement Researchers, Recognizes Growing Real-World Uses of Exotic Phenomena

by Matt Swayne

https://thequantuminsider.com/2022/10/04/nobel-prize-in-physics-goes-to-pioneering-quantum-entanglement-researchers-recognizes-growing-real-world-uses-of-exotic-phenomena/?utm_source=newsletter&utm_medium=email&utm_term=2022-10-24&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Nobel+Efforts+Qunnect+Connects+And+More+Quantum+News

The 2022 Noble Prize in Physics was awarded to three pioneers who conducted experiments on quantum

entanglement. The prize also recognizes that this once esoteric-sounding — and acting — quantum phenomena is becoming the backbone of a rapidly emerging quantum industry. The winners are:

Alain Aspect, born 1947 in Agen, France. PhD 1983 from Paris-Sud University, Orsay, France. Professor at Université Paris-Saclay and École Polytechnique, Palaiseau, France.

John F. Clauser, born 1942 in Pasadena, CA, USA. PhD 1969 from Columbia University, New York, USA. Research Physicist, J.F. Clauser & Assoc., Walnut Creek, CA, USA.

Anton Zeilinger, born 1945 in Ried im Innkreis, Austria. PhD 1971 from University of Vienna, Austria. Professor at University of Vienna, Austria.

The Noble Prize committee awarded the trio the prize for their groundbreaking experiments using entangled quantum states. In entanglement, two particles can behave like a single unit even when they are separated.

According to a statement from the the Nobel Committee, **John Clauser** developed John Stewart Bell's ideas on the theoretical existence of non-locality, often referred to as Bell inequality, that lead to a practical experiment on entanglement. Clauser's eventual measurements supported quantum mechanics by clearly violating a Bell inequality. This ruled out the uses of hidden variables as a way to explain quantum mechanics.

Alain Aspect, addressed an important loophole that remained after Clauser's experiment. Aspect switched the measurement settings once an entangled pair left its source, so that setting could not affect the result.

Among other things, **Anton Zeilinger** and his research group used entangled quantum states to demonstrate quantum teleportation, which makes it possible to move a quantum state from one particle to one at a distance.

A New Kind of Quantum Technology

The committee recognizes that the work of these three researchers is moving from theory to experimentation — and rapidly — to the market.

"It has become increasingly clear that a new kind of quantum technology is emerging. We can see that the laureates' work with entangled states is of great importance, even beyond the fundamental questions about the interpretation of quantum mechanics," says Anders Irbäck, Chair of the Nobel Committee for Physics.

The committee mentions this emerging industry includes quantum computers, quantum networks and secure quantum encrypted communication.

The winners will equally share 10 million Swedish kronor, or about $946,460 US, which means each laureate would receive a little over $315,000.

19.It's 2058. A quantum computer is just another decade away

by Jessica Lyons Hardcastle
https://www.theregister.com/2022/10/03/cloudflare_postquantum_cryptography/

Cloudflare is the first major internet infrastructure provider to support post-quantum cryptography for all customers, which, in theory, should protect data if quantum computing ever manages to break today's encryption technologies.

Starting today all websites and APIs served through Cloudflare support post-quantum TLS based on the Kyber hybrid key agreement. Specifically, the new beta service supports the X25519Kyber512Draft00 and X25519Kyber768Draft00 key agreements using TLS identifiers 0xfe30 and 0xfe31, respectively.

The service is free, and it's on by default — so no need for customers to opt in. It's a hybrid key agreement in that it combines X25519, which is used in TLS 1.3 but still vulnerable to future quantum attacks, and the new, post-quantum Kyber512 and Kyber768.

"That means that even if Kyber turns out to be insecure, the connection remains as secure as X25519," Cloudflare researchers Bas Westerbaan and Cefan Daniel Rubin explained.

Kyber, so far, is the only key agreement that the US National Institute of Standards and Technology (NIST) has officially selected for standardization. NIST plans to finalize this standardization in 2024, and there may be new standards to come.

This, in part, is why Cloudflare is only offering this as a beta service: Kyber will likely change in backwards-incompatible ways before it's finalized, and the integration with TLS hasn't been finalized by the TLS working group, either.

In their blog post, Westerbaan and Rubin pledged to post updates on Cloudflare's post-quantum key agreement support on pq.cloudflareresearch.com and announce it on the IETF PQC mailing list.

Carry on up the Kyber

While quantum computers' ability to crack classic cryptography is still years away — from 15 to 40 years [PDF] in the future to possibly never, depending on who you believe — when and if these machines become powerful enough to decrypt anything on the Internet they will be able to expose state secrets in seconds.

Some infosec and technology consultants have warned that China and others are stealing data now to decrypt later, when quantum computing matures enough to do so.

However, as Cloudflare's researchers outline, deploying post-quantum cryptography comes with risks, too. For starters, it's brand-new cryptography, and sometimes new things that haven't been tested for years break. Case in point: the roll-out of TLS 1.3, which didn't go as smoothly as planned.

"Even though the protocols used to secure the Internet are designed to allow smooth transitions like this, in reality there is a lot of buggy code out there: trying to create a post-quantum secure connection might fail for many reasons — for example a middlebox being confused about the larger post-quantum keys and other reasons we have yet to observe because these post-quantum key agreements are brand new," Westerbaan and Rubin said.

"It's because of these issues that we feel it is important to deploy post-quantum cryptography early, so that together with browsers and other clients we can find and work around these issues," they added.

By deploying well ahead of 2024, Cloudflare and others should have sufficient time to work out any kinks and protect data from quantum attacks, we're told.

Gartner's Mark Horvath, a senior director with the analyst firm, said the move is a "big help" to the industry, "and a great step forward for moving toward a quantum-safe future."

"Post-quantum encryption is expected to have a huge impact on infrastructure, operations and data security over the next decade, and testing protocols like TLS at realistic speeds and volumes helps the industry move forward in a smooth way," Horvath told The Register.

"While dual-signed certificates and other support for post-quantum operations have been introduced occasionally in the past, it's only now that the NIST contest is reaching the standardization phase that we have real tools to work with on issues like protocols that have a huge future impact."

20.There's a New Quantum Computing Record: Control of a 6-Qubit Processor in Silicon

by David Nield
https://www.sciencealert.com/theres-a-new-quantum-computing-record-control-of-a-6-qubit-processor-in-silicon

Another record has been broken on the way to fully operational and capable quantum computers: the complete control of a 6-qubit quantum processor in silicon.

Researchers are calling it "a major stepping stone" for the technology.

Qubits are the quantum equivalents of classical computing bits, only they can potentially process much more information. Thanks to quantum physics, they can be in two states at once, rather than just a single 1 or 0.

The difficulty is in getting a lot of qubits to behave as we need them to, which is why this jump to six is important. Being able to operate them in silicon – the same material used in today's electronic devices – makes the technology potentially more viable.

"The quantum computing challenge today consists of two parts," says quantum computing researcher Stephan Philips from the Delft University of Technology in the Netherlands. "Developing qubits that are of good enough quality, and developing an architecture that allows one to build large systems of qubits."

"Our work fits into both categories. And since the overall goal of building a quantum computer is an enormous effort, I think it is fair to say we have made a contribution in the right direction."

The qubits are made from individual electrons fixed in a row, 90 nanometers apart (a human hair is around 75,000 nanometers in diameter). This line of 'quantum dots' is placed in silicon, using a structure similar to the transistors used in standard processors.

By making careful improvements to the way the electrons were prepared, managed, and monitored, the team was able to successfully control their spin – the quantum mechanical property that enables the qubit state.

The researchers were also able to create logic gates and entangle systems of two or three electrons, on demand, with low error rates.

Researchers used microwave radiation, magnetic fields, and electric potentials to control and read electron spin, operating them as qubits, and getting them to interact with each other as required.

"In this research, we push the envelope of the number of qubits in silicon, and achieve high initialization fidelities, high readout fidelities, high single-qubit gate fidelities, and high two-qubit state fidelities," says electrical engineer Lieven Vandersypen, also from the Delft University of Technology.

"What really stands out though is that we demonstrate all these characteristics together in one single experiment on a record number of qubits."

Up until this point, only 3-qubit processors have been successfully built in silicon and controlled up to the

necessary level of quality – so we're talking about a major step forward in terms of what's possible in this type of qubit.

There are different ways of building qubits – including on superconductors, where many more qubits have been operated together – and scientists are still figuring out the method that might be the best way forward.

The advantage of silicon is that the manufacturing and supply chains are all already in place, meaning the transition from a scientific laboratory to an actual machine should be more straightforward. Work continues to keep pushing the qubit record even higher.

"With careful engineering, it is possible to increase the silicon spin qubit count while keeping the same precision as for single qubits," says electrical engineer Mateusz Madzik from the Delft University of Technology.

"The key building block developed in this research could be used to add even more qubits in the next iterations of study."

The research has been published in *Nature*.

21.UK startup Oxford Quantum Circuits (OQC) is to install its quantum computer in a data centre, the first such co-location deal.

by Andre Rousselot
https://www.eenewseurope.com/en/oqc-in-first-quantum-computer-co-location-data-centre-deal/

The deal marks a significant step in moving quantum computing from a lab environment into a fully managed, industry-ready environment with the security, interconnectivity, network bandwidth, and redundant infrastructure that will be needed as the technology matures.

The deal with Cyxtera is the world's first integration of a quantum computer in a colocation data centre, says OQC, although its quantum computer and others are available remotely through Amazon's Bracket public cloud service or through QC's private cloud.

OQC is one of the best funded quantum computer startups in Europe and has an 8qubit quantum computer called Lucy. It 4 qubit system, called Sophia, is being used by Quantinuum for a private cloud service.

Customers using Cyxtera's UK data centres will be able to access OQC's quantum computer at a data centre in Reading via the Cyxtera Digital Exchange, reducing latency times for quantum algorithms and applications.

"For quantum computing to be genuinely accessible and fully realize its potential as a technology, it must seamlessly integrate within businesses' current computing and data management infrastructure. At this stage, it simply cannot work in isolation. Thanks to this pioneering partnership, we will give Cyxtera's customers direct access to our latest quantum computer—within their data centres, at the click of a button—without making any changes to their operations," said Dr. Ilana Wisby, Chief Executive Officer, OQC.

"Quantum computing will enable organizations across a wide range of industries to access unprecedented calculation speed and deeper analytical capabilities," said Randy Rowland, Chief Operating Officer, Cyxtera. "We're thrilled to partner with OQC, providing our customers access to the U.K.'s most advanced quantum computing platform."

OQC will also join the Cyxtera ecosystem of service providers, giving access to 2,300 enterprise and government customers

22.Cloudflare's post-quantum cryptography protects almost a fifth of the internet

by Tim Keary
https://venturebeat.com/security/cloudflare-post-quantum-cryptography/

The countdown to Y2Q, the day when quantum computers can decrypt public key algorithms, is on. While researchers don't know exactly when this will happen, the Cloud Security Alliance (CSA) estimates this could be as soon as April 14, 2030.

Although many organizations are waiting for post-quantum threats to become tangible before taking action against them, other providers like Content Delivery Network (CDN) giant Cloudflare are diving straight in and responding with quantum-safe solutions.

Today, Cloudflare announced it has launched post-quantum cryptography support for all websites and APIs served through its network. Essentially, this will introduce quantum computer-proof encryption for all sites using Cloudflare, which accounts for 19.1% of all websites according to W3Techs.

Above all, the fact that a prominent security vendor like Cloudflare is committing to post-quantum cryptography highlights that enterprises should take the threat of malicious quantum computers seriously.

Countdown to Y2Q: Why the time for post-quantum is now

The announcement comes shortly after Cloudflare announced the release of the first Zero Trust SIM to secure mobile devices, and a $1.25 billion funding program designed to help startups scale their businesses.

Now Cloudflare is the first content delivery network to support post-quantum TLS based on NIST's chosen cyber algorithm. While this decision may seem premature, it's at the perfect time to prevent harvest now, decrypt later style attacks.

Currently, threat actors and nation-states can collect encrypted data with the intention to decrypt it once quantum computing advances to the level necessary to decrypt it.

"There is an expiration date on the cryptography we use every day. It's not easy to read, but somewhere between 15 or 40 years, a sufficiently powerful quantum computer is expected to be built that'll be able to decrypt essentially any encrypted data on the Internet today," wrote Cloudflare in the announcement blog post.

"Starting today, as a beta service, all websites and APIs served through Cloudflare support post-quantum hybrid key agreement. This is on by default; no need for an opt-in. This means that if your browser/app supports it, the connection to our network is also secure against any future quantum computer," the post said.

