Crypto News

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

October 01, 2023

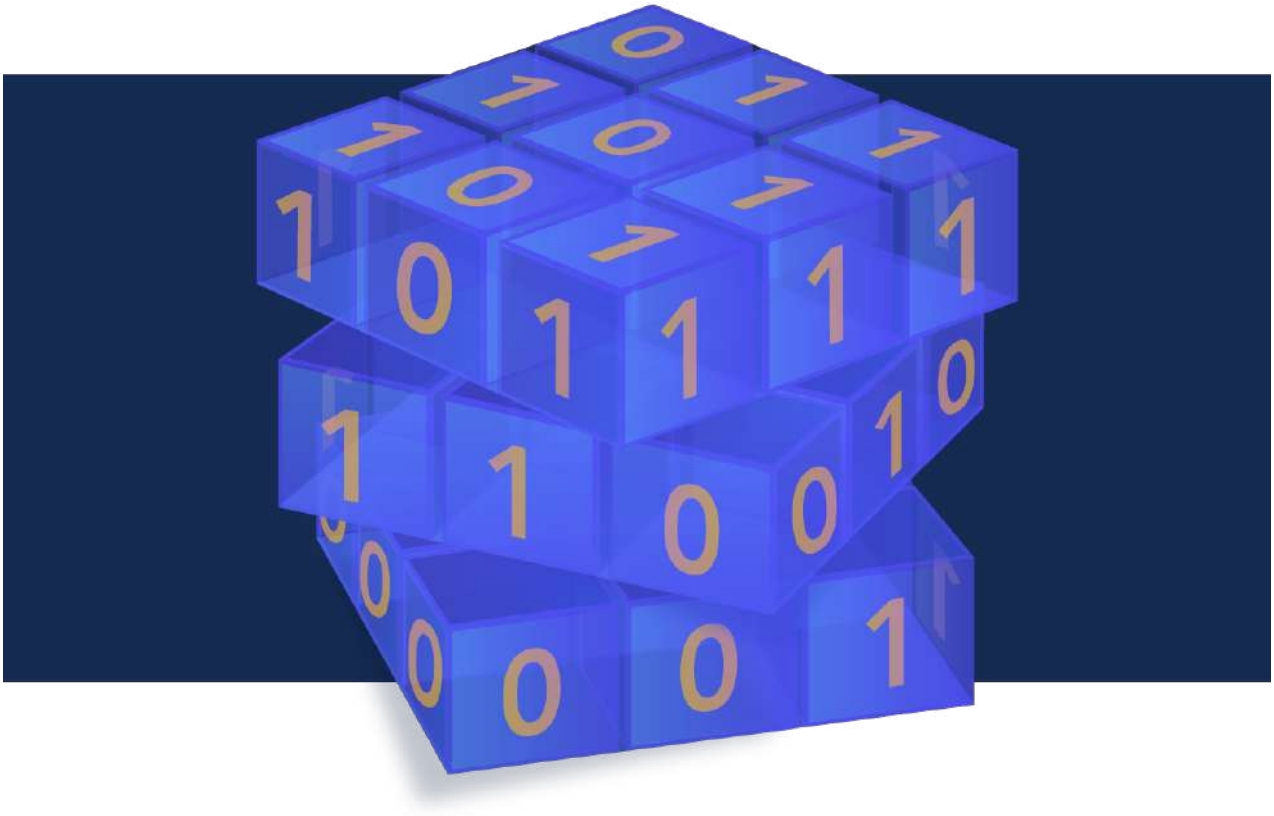


TABLE OF CONTENTS

Editorial

You'll often hear us in the Quantum-Safe Security Working Group state that the quantum threat is not only real but that many organizations have yet to start their quantum journey. What professionals in cybersecurity and quantum computing struggle with is being heard when they push organizations to proactively address the quantum threat. What may bring more attention to the quantum threat and catch the attention of organizations is the development of cryptanalytically relevant quantum computers (CRQCs) which will be done in anything but silence or a vacuum. CRQCs are what will run Shor's algorithm and "break the encryption" we use today. The author of article 16 lists out the four main reasons why there will be "noise", with one of them simply being that companies making quantum computers will eventually need to attract customers through advertising. After all, any scientific research and discovery needs funding to make it all work and to keep that work going. Maybe all of this "noise" will help organizations see that they need to get started now to be quantum ready.

Next, what better place to talk about cryptography (true full form of the term "crypto") than in relation to another technology that has recently borrowed the term "crypto" – cryptocurrency. More specifically, blockchain technology. Semantics aside, cryptography is the backbone of blockchain technology. If you'd like to learn more details about data security as it relates to blockchain and cryptography, scroll down to article 13. With the inevitable impacts of CRQCs mentioned previously, now would be the right time to start asking your cryptocurrency and cryptocurrency exchanges about how they plan to protect your assets. Why? Because financial giants dealing with traditional currency are already getting started. In article 9, you can get more details about Mastercard's journey towards a post-quantum world. They have chosen to go down the path of quantum key distribution (QKD) which is one of the solutions that organizations can embrace to counter the threat to public-key encryption. Navigate to the article to get more details. As always, happy reading!

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

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

1.Post-Quantum Cryptography: Finally Real in Consumer Apps?

by The Hacker News
https://thehackernews.com/2023/09/post-quantum-cryptography-finally-real.html

Most people are barely thinking about basic cybersecurity, let alone post-quantum cryptography. But the impact of a post-quantum world is coming for them regardless of whether or not it's keeping them up tonight.

Today, many rely on encryption in their daily lives to protect their fundamental digital privacy and security, whether for messaging friends and family, storing files and photos, or simply browsing the web. The question experts have been asking for a long time, with their eye on the advances in quantum computing, is, "How long before these defenses fail?"

The ticking clock of quantum computing

One set of researchers is already sounding the alarms, claiming that they've found a way to break 2048-bit RSA encryption with a quantum computer. While the claims may be premature, they hint toward a scary future that is perhaps closer than we once thought. Breaking RSA encryption would represent a massive privacy and security vulnerability for virtually every aspect of our digital lives—a master key for all our digital data.

And it's not just our future data and communications at risk. The breaching of modern encryption protections can have deep retroactive impact as well, with the possibility that attackers are harvesting data now with the hope of decrypting it in the future.

"We know for a fact that store-now-decrypt-later attacks are happening right now, and their frequency will only increase the closer we get to delivering a fault-tolerant quantum computer," says David Joseph, a research scientist at Sandbox AQ. "Once encrypted data has been exfiltrated, there is no way to protect it from future decryption and exploitation."

Simply put, while your encrypted messages may be safe and private today, if someone captures them and holds onto them until they get access to a quantum computer, they'll be able to decrypt and read them in the future.

The emergence of post-quantum cryptography

Post-quantum cryptography (PQC) refers to cryptographic algorithms that are resistant to attacks by both classical (i.e., the non-quantum ones we use today) and quantum computers. These algorithms are based on mathematical problems that are believed to be computationally hard for both types of computers. They serve as a backup plan to ensure that our data remains secure in a future where powerful quantum computers exist.

While PQC has been a topic of research and development for many years, it's only just now starting to see early applications in the consumer protection space. This is due to a number of factors, including the increasing maturity of PQC algorithms and the growing awareness of the threat of quantum attacks. Last month, for example, Chrome just began supporting a PQC algorithm, though it will not be in wide use yet and will be dependent on broader ecosystem support.

Hybrid cryptography for comprehensive defense

One of the challenges of post-quantum cryptography is that it's still in the early stages of development, lacking the track record of the widely used and time-proven classical cryptography of today. That's where hybrid cryptography comes in, providing a two-layered shield of sorts.

"A hybrid approach means that users are safe from attacks by classical computers without relying on post-quantum algorithms, and they also have the best chance we know of today of being safe from attacks by quantum computers," explains Peter Membrey, Chief Engineering Officer at ExpressVPN. "Post-quantum algorithms are still relatively new and less battle-tested. By leaving classical cryptography in the hands of existing tried-and-true standards, we can ensure any unforeseen issues with post-quantum algorithms don't impact the security or integrity of the broader cryptographic infrastructure—and by extension the security of users."

As messaging app Signal recently explained in an announcement about quantum-resistant encryption, instead of replacing any existing classical cryptography, they use PQC to "[augment] existing cryptosystems such that an attacker must break both systems in order to compute the keys protecting people's communications."

The future of PQC in consumer applications

Recent advances in PQC in consumer apps are the vanguard of a new era in cybersecurity and a sign that the tech industry is taking quantum threats seriously. As quantum computing moves from science fiction to reality, the question isn't whether we need post-quantum cryptography—it's how quickly we can make it a standard feature in our digital lives. The clock is ticking, and soon more consumers will be asking not just what their apps are doing to protect their data today, but also how they're preparing for the threats of tomorrow.

2.Fully homomorphic encryption revolutionises healthcare data privacy and innovation

https://www.openaccessgovernment.org/fully-homomorphic-encryption-revolutionises-healthcare-data-privacy-and-innovation/167103/

Chief Technology Officer at Zama **Dr Pascal Paillier** talks to Open Access Government about why privacy in healthcare matters, the privacy barriers faced by the industry and how Fully Homomorphic Encryption (FHE) could help

Q: Tell us a bit about you and your area of expertise

I'm currently the Chief Technology Officer (CTO) and co-founder of Zama, a startup that powers machine learning and other applications with homomorphic encryption to ensure data privacy.

I am a researcher and entrepreneur specialised in cryptography and have more than 27 years of experience in the security industry, with a specific interest in designing and developing secure cryptographic

primitives (homomorphic encryption, anonymous credentials, etc.) as well as crypto software for embedded architectures such as smart cards.

I have a PhD in cryptography from Telecom Paris and am a member of IACR. I also am an expert at ISO, contributing to international standardisation efforts for cryptography.

Q: Why do you think data privacy in healthcare is considered a critical concern, and what are the potential consequences of data breaches in this sector?

Data privacy in the healthcare sector is a huge concern, primarily because it involves highly sensitive personal information. Patients entrust healthcare providers with their most intimate health records, and any breach of this trust can have profound consequences; unauthorised access to medical records, for example, can expose personal and medical details, leaving individuals vulnerable to identity theft, fraudulent activities, or other malicious actions.

Financial losses are another major consequence. Data breaches can result in substantial financial burdens for both healthcare organisations and the individuals affected, legal actions, regulatory fines, and efforts to mitigate the breach's impact.

The reputation of healthcare providers is also on the line. When patients believe their confidential information is not adequately protected, trust in the healthcare system simply erodes. Patients may become hesitant to share sensitive information with their healthcare providers, potentially compromising the quality of care they receive.

Q: What are the existing barriers and challenges to maintaining data privacy in healthcare?

One major issue is the lack of interoperability among healthcare systems, leading to data silos that hinder secure data sharing and integration across institutions. Legacy systems – still in use in many healthcare organisations – may lack modern security measures and can be more vulnerable to cyberattacks, which, due to the value of patient data, are **rising at an alarming rate in healthcare**.

Human error is also a concern. Data breaches in healthcare often result from mistakes such as sending patient information to the wrong recipient, mishandling physical records, or falling for social engineering attacks like phishing. Inadequate training on data security best practices can contribute to these errors, and determining data ownership and obtaining informed consent for data sharing can be a complex business.

Many healthcare organisations also rely on third-party vendors for services like cloud storage, which can introduce new security risks, while balancing the need for collaborative research with privacy concerns is another challenge, especially when sharing patient data among multiple institutions and researchers. And finally, resource constraints, particularly in smaller healthcare organisations, can limit their ability to implement robust data privacy measures.

Q: Can you explain the basic principles of Fully Homomorphic Encryption (FHE) and how it differs from other encryption methods?

With traditional encryption, you essentially lock up your data in a secure "box" (the encrypted form) using a key. To do anything useful with the data, like performing calculations or searches, you must first "unlock" or decrypt it using the key.

Once decrypted, the data is vulnerable, and if someone gains access to it during this phase, your privacy is compromised.

FHE, on the other hand, takes encryption to the next level by allowing you to perform operations directly

on the encrypted data without revealing the underlying information. Imagine your data is in a secure "box," and with FHE, you can perform operations on the data while it's still inside the locked box.

The result of these operations is also encrypted, preserving the privacy of the data at every step. Only when you're done with all the calculations and ready to see the final result do you unlock the box through decryption to reveal the output?

We're already seeing Fully Homomorphic Encryption medical potential come to life, and we have started to demonstrate the technology's practical application in this area through a **demo** that's currently available on Hugging Face.

Q: In what ways can FHE address the challenges of data privacy in healthcare, particularly with regard to secure information sharing and analysis?

In the context of healthcare, Fully Homomorphic Encryption offers a transformative solution to the challenges of data privacy in the industry, especially in the context of secure information sharing and analysis. With FHE, medical organisations can perform computations directly on encrypted data, allowing them to securely share or collaborate on research, diagnosis, and treatment planning without the risk of exposing sensitive patient information.

Essentially, FHE acts as a secure intermediary, allowing multiple parties to work with sensitive data without compromising its privacy.

Q: What are the benefits of this approach?

Eliminating the need for data decryption during collaboration not only enhances security but also streamlines the research and decision-making process. It fosters trust among healthcare providers and institutions, encouraging active participation in improving patient care. This is why I am expecting to see a wide adoption of FHE in healthcare in the coming years.

Q: Can FHE contribute to improving patient-provider relationships?

Yes, it plays a pivotal role in empowering patients to have greater control over their personal health data because they no longer need to choose between data security and quality healthcare. With FHE, patients can securely share their encrypted health information with healthcare providers, allowing for accurate diagnoses and tailored treatment plans while safeguarding privacy.

Patients are more likely to actively engage in managing their health when they know their sensitive information is protected. The trust established through FHE ensures that patients feel comfortable sharing their health-related data with healthcare professionals, leading to improved communication and better healthcare outcomes.

Q: What regulatory and compliance issues does Fully Homomorphic Encryption help healthcare organisations address, and how does it impact their ability to use data for research and analytics?

FHE helps healthcare organisations address various regulatory and compliance issues, particularly those related to data protection laws such as GDPR and HIPAA. FHE ensures that data remains encrypted throughout processing, even during research and analytics. This adherence to strict data protection regulations is crucial for healthcare organisations to avoid legal consequences and maintain public trust.

The impact of FHE on the ability to use data for research and analytics is significant. It allows healthcare organisations to harness the power of their data while remaining compliant with regulatory frameworks. By securely performing computations on encrypted data, FHE enables innovative research and analytics without compromising patient privacy.

It opens up new possibilities for deriving valuable insights from healthcare data while adhering to stringent legal requirements. In other words, FHE gives all institutions the superpower of full legal compliance by design by completely eliminating the risk of data breach so that they do not have to care about that anymore.

Q: What are the current limitations or challenges associated with implementing FHE in healthcare settings, and what steps are being taken to overcome these obstacles?

Implementing FHE in healthcare settings is not without its challenges. One significant limitation is the computational overhead associated with FHE, which can slow down data processing and analysis. This is a practical challenge that requires significant research efforts to optimise Fully Homomorphic Encryption algorithms and make them almost as efficient as usual data processing.

As we speak, cryptography and computer science experts across academia and industry are collaborating to develop faster and more practical FHE implementations by releasing cutting-edge software tools and, soon, hardware acceleration. These advancements aim to make FHE more accessible for real-world healthcare scenarios. Additionally, the healthcare industry is actively exploring ways to integrate Fully Homomorphic Encryption into existing systems and workflows to maximise its benefits while addressing these limitations.

3.Preparing for the post-quantum cryptography environment today

by Christopher Burgess
https://www.csoonline.com/article/653471/preparing-for-the-post-quantum-cryptography-environment-today.html

It's a mistake to put off the creation of precautions against quantum threats, no matter how far in the future you might think quantum computing will become a reality.

The thought of quantum computing may elicit a shrug from many a CISO who has enough on their plate already and has decided that's an issue for the future. My take: get into the conversation, as it is your entity that will be affected sooner or later when post-quantum cryptography becomes a possibly concerning reality.

Quantum cryptography must become a concern for the cybersecurity expert as we (as a community) "don't tend to prioritize the things that are important until they become urgent," Jaya Baloo, CSO at Rapid 7, tells CSO. "It's precisely why we need to start getting ready today for the arrival of quantum computers jeopardizing our current cryptography."

That advice got my attention. Baloo went on to summarize three steps that every CISO should be taking today:

1. **Know thyself**. Assess and inventory current cryptographic assets and understand their use in our enterprises.

2. **Find opportunities.** Look for opportunities that will eventually allow you to transition to quantum-safe technologies.

3. **Implementation**. Have in place a steady cycle of implementing, monitoring, and testing that makes sure that you have some operational assurance you will be ready when quantum becomes a reality.

She concludes with a sage observation: "It is helpful to take the lessons learned in this step [3 above] and share them within your trusted security communities to make sure that we all level up together and encourage each other as well as our vendors to help us in the journey of quantum readiness. Only when we secure our ecosystems can we enjoy the benefits of quantum computing without continually worrying about the risks to information security."

Baloo was not alone in her opinions. Nils Gerhardt of Utimaco spoke to me at the most recent RSA about the need to engage in the first two of Baloo's steps to get ahead of the proverbial curve. "We need seamless transitions to occur" was his primary message. While Joseph Carson of Delinea pointed to the need to engage with those steps in looking for opportunities to implement quantum-resistant solutions.

Read the US Government's how-to guide to quantum preparedness

Then we have the US government publishing in late August 2023 its preparedness guide with advice from NIST, CISA and NSA on "how to prepare now."

"Post-quantum cryptography is about proactively developing and building capabilities to secure critical information and systems from being compromised through the use of quantum computers," Rob Joyce, Director of NSA Cybersecurity, writes in the guide.

"The transition to a secured quantum computing era is a long-term intensive community effort that will require extensive collaboration between government and industry. The key is to be on this journey today and not wait until the last minute."

This perfectly aligns with Baloo's thinking that now is the time to engage, and not to wait until it becomes an urgent situation.

The guide notes how the first set of post-quantum cryptographic (PQC) standards will be released in early 2024 "to protect against future, potentially adversarial, cryptanalytically-relevant quantum computer (CRQC) capabilities. A CRQC would have the potential to break public-key systems (sometimes referred to as asymmetric cryptography) that are used to protect information systems today."

The guide points to four steps (not surprisingly, they also align nicely with Baloo's advice).

1. **Establish a Quantum-Readiness Roadmap.** Employ proactive cryptographic discovery to identify the organization's current reliance on quantum-vulnerable cryptography.

2. **Engage with technology vendors to discuss post-quantum roadmaps.** Future contracts will ensure "new products will be delivered with PQC built in." In addition, the mitigation strategies of vendors may be of utility to entities as they plan their own pathways to mitigation. This engagement should also include supply-chain discussion as well as the vendor technology responsibilities.

3. **Conduct an inventory to identify and understand cryptographic systems and assets.** This means one must put together a comprehensive cryptographic inventory of current systems.

4. **Create migration plans that prioritize the most sensitive and critical assets.** The organizations' risk assessments and pathways to mitigation are not static.

When all voices are singing the same tune from the same choir loft, one should take note. CISOs should designate a point for their quantum migration project that will take place over a number of years. The first steps as recommended by the US government, Bayoo, Carson, and Gerhardt are all the same – figure out what you have and take inventory.

Begin to sunset PQC-vulnerable systems now

Then, resources permitting, follow the guidance of Bayoo and begin sunsetting those cryptographic systems identified as PQC vulnerable and replacing them as the opportunity presents itself with cryptographic systems which have been identified as being PQC resilient. This is not a light lift, it is indeed a heavy lift, yet a necessary lift.

For the skeptics amongst us, and we all have a vein or two of skepticism within, I commend to your attention the opinion piece of December 2021: "Collect today, decrypt tomorrow: How Russia and China are preparing for quantum computing" and note the parallelism within the US government bulletin of August 2023 how adversaries will adopt a strategy of "catch now, break later -- or, harvest now, decrypt later" operations.

Sitting on the sidelines and waiting is not an option

4.Taiwan needs to close learning gap in post-quantum cryptography, says expert in field

by Sophia Yang and Jennifer Lin
https://www.taiwannews.com.tw/en/news/5007408

Not many people are dedicated to the study and application of quantum-resistant or post-quantum cryptography (PQC) in Taiwan, but one young data scientist at Academia Sinica believes engagement in the field is attainable, despite its apparent complexity and knowledge barrier.

Assistant Research Fellow at Academia Sinica's Research Center for Information Technology Innovation, Tung Chou (周彤), has for the past decade been focused on the field of quantum-resistant encryption. He started as a programmer before delving into quantum-safe cryptography.

Chou suggested that those with an interest in cryptography should begin with a branch of knowledge they specialize in. For example, Chou said, mathematicians can leverage their expertise in mathematical analysis, while broadening knowledge from research papers outside their area of specialization.

"I invested a significant amount of time in reading research papers, integrating theory and practice to eventually nail down my focus in post-quantum cryptographic research," Chou said.

He encouraged cryptography researchers to step out of their comfort zone and delve into diverse disciplines and topics. "I reached out to professors of different specialties on various cryptography topics throughout my graduate studies, invested a significant amount of time in reading research papers, exposed myself to various disciplines which I am not familiar with, and that altogether inspired me to cre-

ate efficient cryptographic algorithms. It is a rewarding journey," he said.

Chou believes that in Taiwan, Academia Sinica researchers have been the most dedicated group studying PQC, but he hopes more new blood, outside the country's top research institution, is brought into the field. His observation is based on his participation seven years ago in an American cryptography contest when the contestants were diverse and came from both academia and industry.

PQC learning journey

Chou's learning journey consisted of two phases: master's degree studies under Academia Sinica Research Fellow Yang Bo-yin (楊柏因), who guided him to solve multivariate polynomial equations intended for launching attacks on cryptosystems, including multivariate cryptography, and PhD studies in the code-based public-key cryptosystem introduced by McEliece in 1978. In addition, in 2017, he competed on a team at the Post-Quantum Cryptography Standardization competition, hosted by the National Institute of Standards and Technology (NIST). His role was to optimize software and improve the public-key generation algorithm.

"The McEliece cryptosystem has remained remarkably stable over 40 years, surviving numerous attacks and garnering confidence among academics and experts in cryptography. It was naturally the first choice that many NIST's contesting quantum-resistant cryptography algorithms have leveraged over the past 20 years, though there were variations made to compress public keys," Chou said.

"The conservative code-based cryptographic algorithm is known for its fast speed of executing the encryption and decryption, and it is applicable on desktop and mobile devices," he added.

However, McEliece has a drawback — its key sizes are very large. Chou explained that in public key cryptography, two keys are used. "One key is used for encryption (public key), and another is used for decryption (private key)." The one for encryption (public key) can be accessed by anyone for viewing and encrypting, while the encrypted data can be sent back to the holder of the private key.

In general, the size of the public key is large and comes with many restrictions while encrypting, Chou said. "The public key size is around one megabyte, so transmitting public keys can be expensive for mobile devices," he said.

When asked whether the key size can be trimmed to solve the problem, Chou said it remains a topic of debate. "There have been NIST PQC contestants trying to shorten the large public key size by modifying its mathematical structures, but whether it comes at the expense of its safety is still unknown," he said.

However, Chou said he prefers that the key remains at its current length. The algorithm has been unbreakable for over 40 years, Chou said, which demonstrates the cryptography community's unshakable belief in it.

"I do not know whether the NIST would announce McEliece as a cryptographic standard to resist the advent of quantum computers, but I do hope the post-quantum cryptosystems can be extensively applied in various devices in the future," he said.

Better early than late

In Taiwan, the ecosystem is still being built up as the talent pool for post-quantum cryptography has room for improvement, and the legal hurdles should be removed to make the ecosystem robust, Chou said. In Europe, on the other hand, a strong post-quantum cryptography ecosystem already exists, which gathers mathematicians, algorithm experts, and those who are good at securing devices from hackers, from stealing data on encrypted mobile devices.

There are businesses dedicated to promoting PQC, which has been around for decades. Thanks to their efforts, people living in Taiwan, unknowingly, enjoy financial and internet services secured by cryptography, such as accessing the internet and using ATMs.

However, Chou warned there is a lot of software and hardware that still adopts outdated cryptographic algorithms, putting their sensitive data at risk. He called on businesses and government institutions for early migration to quantum-safe cryptography to keep data safe from quantum algorithm-based attacks in the future.

He uses the Hypertext Transfer Protocol Secure (HTTPS) as an example, which is an encrypted and secure version of the HTTP protocol, saying HTTPS is, however, not encrypted based on quantum-safe technology.

Chou recommended government and education institutions, businesses, and big tech companies assess their cryptographic systems, adapt their hardware and software, and phase out old systems for new ones, in particular, those storing sensitive and important data. It will be too late to migrate to the new cryptographic system when quantum computers become a reality.

Chou said that although some people might think that quantum computers will be ready in 10 or 20 years, and they can start to work on the migration then, "it is a problematic mindset," he warned. "We believe that bad actors are gaining access to currently encrypted data and would decrypt it at a later time using a quantum computer," Chou said.

He advises all parties to rethink their data security and decide what should be protected over a longer time frame and begin planning for migration to a quantum-proof space.

Chou said, "As a cryptography professional, I do hope everyone's data can be protected by this powerful algorithm, regardless of their socioeconomic status. The PQC should be extensively introduced into all devices nationwide as early as possible."

"I understand there is a long way to go because the cryptographic protocol is not Taiwan's strong point, but we have to run fast," Chou concluded.

5.Post-Quantum Cryptography Coalition Launches

by Business Wire
https://www.galvnews.com/news_ap/business/post-quantum-cryptography-coalition-launches/article_27f03be8-1215-5d83-a6c6-cdd4465460b0.html?block_id=531919

The data we're encrypting online today—from financial and personal identification information to military operations and intelligence data—could be quickly decrypted in the future by an adversary with access to a cryptographically relevant quantum computer. To drive progress toward broader understanding and public adoption of post-quantum cryptography (PQC) and the National Institute of Science and Technology's (NIST) PQC algorithms, a community of technologists, researchers, and expert practitioners launched the PQC Coalition. Founding coalition members include IBM Quantum, Microsoft, MITRE, PQShield, SandboxAQ, and University of Waterloo. "Quantum computers may not be here yet, but their impending arrival is already bringing both opportunities and threats to

national and economic security," said Charles Clancy, chief futurist and senior vice president, MITRE, and general manager, MITRE Labs. "Government and industry need to move together with urgency so that sensitive data and communications are not vulnerable to exposure in the future."

"The PQC Coalition is well-positioned with both the knowledge and expertise to facilitate a smooth and rapid global transition to PQC and the adoption of crypto-agility for widespread quantum resistance," said Jen Sovada, president of the public sector at SandboxAQ. "As a charter coalition member, SandboxAQ will leverage its deep public- and private-sector connections to create broader issue awareness, drive development and implementation of PQC solutions, and help streamline the process for organizations to migrate to PQC."

"IBM has played a key role in driving the development of the new NIST algorithms and has also begun implementing the algorithms in our own technologies and client solutions. Now the time has come to look at the greater industry perspective, and we are delighted to be a charter member of this coalition," said Mike Osborne, CTO, Quantum Safe, IBM Quantum.

"In the ever-evolving landscape of cybersecurity and as quantum technology continues to advance and change the world, our commitment to the security of our products and customers has never been stronger," said Inbar Badian, Quantum Safe Program Lead, Office of the CTO, Microsoft Security. "Joining the Post-Quantum Cryptography Coalition is another example of our dedication to being a trusted partner across industry and government towards building a quantum-safe future together."

Ben Packman, senior vice president, PQShield, added, "PQShield is proud to be a founding member of the PQC Coalition, where our expertise and already commercially deployed PQC hardware and software can be leveraged, alongside fellow members, to help to modernize the vital systems and components in the world's technology supply chain—a key building block to support both government and enterprise migration plans globally."

"The research community has been working for the past decade to design and evaluate post-quantum cryptography algorithms that we can rely on," said Douglas Stebila, professor at the University of Waterloo and co-founder of the Open Quantum Safe open-source software project. "The PQC Coalition will advance the deployment and adoption of these algorithms by bringing together key players across industry, academia, and government."

The PQC Coalition will apply its collective technical expertise and influence to facilitate global adoption of PQC in commercial and open-source technologies. Coalition members will contribute their expertise to motivate and advance interoperable standards and technical approaches and step forward as knowledgeable experts in providing critical outreach and education. With the collective energies of the coalition, maturing technology and readying the ecosystem for the post-quantum transition can be worked in parallel with NIST and alongside the National Cybersecurity Center of Excellence's PQC Migration Project to provide comprehensive information, technology, and guidance for the community.

The July 2022 selection by NIST of four PQC algorithms represented the first step toward enabling a PQC migration. In August 2023, NIST released draft standards for three of the four algorithms. A draft standard for FALCON, the fourth algorithm, is expected to be released in 2024. Moving from developing and assessing the theory behind these algorithms toward transition planning and standardization and integration of the algorithms into libraries, protocols, and commercial technology is no small task. Preparing for a PQC transition includes developing standards for the algorithms; creating secure, reliable, and efficient implementations of those algorithms; and integrating the new post-quantum algorithms into cryptographic libraries and protocols. The defensive value of post-quantum cryptography to the world depends on all these preparatory steps, plus the actual deployment of PQC in computer systems and products.

The coalition initially will focus on four work-streams:

- Advancing standards relevant to PQC migration,
- Creating technical materials to support education and workforce development,
- Producing and verifying open-source, production-quality code, and implementing side-channel resistant code for industry verticals, and
- Ensuring cryptographic agility.

6.Role of academic institutions in the National Quantum Mission

by Dr. Angshuman Karmakar
https://www.expresscomputer.in/guest-blogs/role-of-academic-institutions-in-the-national-quantum-mission/103976/

The National Quantum Mission (NQM) stands as a monumental initiative orchestrated by the Government of India, aimed at fostering a dynamic and innovative quantum technology ecosystem. Spanning the period from 2023-24 to 2030-31, this mission seeks to position India as a vanguard in quantum science and technology on the global stage.

Quantum technology, a swiftly evolving domain, holds the potential to reshape industries ranging from computing and communication to healthcare. Quantum computers, for instance, possess the prowess to solve challenges that defy classical computation. Quantum communication networks, meanwhile, promise invulnerable and secure exchanges.

Within the next eight years, the NQM targets developing intermediate-scale quantum computers with 50-1000 physical qubits in various platforms like superconducting and photonic technology. The mission entails investment in research and development of quantum technologies, coupled with the creation of quantum-powered products and services. Notably, this mission is designed to cultivate a skilled workforce in quantum science and technology, while fostering international collaborations to expedite the advancement of future technologies that will soon transform into present realities.

As the NQM unfurls, academic and research institutions stand primed to collaborate and contribute, catalysing quantum technology development and propelling economic growth. For example, the Indian Institute of Technology Kanpur (IITK) delves into Quantum Cryptography, a domain crucial for safeguarding data confidentiality, integrity, and network security. Despite the numerous advantages of quantum computing, such as accelerated drug discovery, accurate weather forecasts, faster artificial and machine learning
applications, and more, quantum cryptography, which focuses on computer security, remains its single most crucial element.

IITK has undertaken extensive research on areas like post-quantum cryptography that uses protocols that can run on existing computing devices and use already established communication channels. There is a lot of ongoing work on computer security, which is the most significant implication of quantum computing with its potential to break commonly used encryption protocols.

Currently, post-quantum cryptography research focuses on analysing physical attacks on cryptographic schemes to propose countermeasures. It includes testing the performance and deployment of countermeasures on a variety of platforms like graphics processing units (GPUs) and small sensors or microcontrollers.

The ongoing research positions the institute to play a pivotal role in the formulation of post-quantum cryptographic standards, ensuring a seamless transition from existing norms and guarding against impending threats. Such contributions reinforce India's prowess in quantum technologies and cybersecurity, rendering the nation enticing for foreign investment and talent.

This drive dovetails with the aspiration to bolster India's scientific and technological competency while harnessing quantum technologies to enhance healthcare, communication, and disaster management, thereby fortifying national security and interests.

Notably, IITK also boasts a distinguished track record in quantum physics, quantum computing, and quantum communication research. Its commitment to pioneering studies in these arenas significantly contributes to the emergence of novel technologies in the field.
Harnessing their scientific and engineering expertise, top-tier institutions can pave the way for quantum-enabled products and services such as quantum computers, communication networks, and sensors. IITK has already forayed into quantum computing courses, which are instrumental in training the forthcoming cohort of scientists and engineers, essential for the innovation and utilisation of quantum technologies.

Collaboration, a bedrock of progress, sees India's premier institutions uniting with their global counterparts, propelling quantum technology advancement and propelling the nation toward global leadership in the field. Beyond these realms, academic institutions hold the potential to further expedite the NQM, a transformative opportunity for India to ascend as a quantum superpower. The momentum of the mission can be galvanised by organising conferences and workshops focused on quantum technologies, provision of technical support to quantum technology startups, advocacy for quantum technology advancement at national and international forums, and cultivating awareness among students and the public.

As India propels forward on the NQM trajectory, it is the synergy between government initiatives and academic brilliance that will steer the nation toward realising its quantum ambitions. With an unyielding commitment to innovation, collaboration, and education, India's academic institutions serve as the fulcrum for propelling quantum technology from theory into transformative reality.

7.QuickLogic and Xiphera Team Up on Post-Quantum Cryptography on eFPGAs

by QuickLogic Corp
https://www.eetasia.com/quicklogic-and-xiphera-team-up-on-post-quantum-cryptography-on-efpgas/

QuickLogic Corp. is partnering with Xiphera to implement its xQlave quantum-secure cryptographic IP cores on QuickLogic's eFPGA architecture. This partnership provides architects with a path towards securing their assets against the quantum threat, enabling them to stay one step ahead in the evolving landscape of cyber threats.

With the rapid development of quantum computers and the increasing threat they pose to information and network security, the need for robust cybersecurity measures has become more crucial than ever. Xiphera answers the quantum-threat with its xQlave family of PQC IP cores. The family includes ML-KEM (Kyber) and ML-DSA(Dilithium)—primary PQC algorithms in the PQC standard draft of the National Institute of Standards and Technology (NIST)—with logic-only implementations. Together, these IP cores provide quantum-secure key exchange, digital signature and authentication.

eFPGA technology offers two key benefits to implementing hardware security —distributed on-chip programmability, and the ability to parallelize intensive algorithmic computation requirements. This enables the eFPGA IP cores to offload heavy cryptographic operations from processor/software implementations, resulting in superior boot up and key calculation times. Furthermore, keys and secrets can be isolated from the rest of the system providing secure access only to trusted components. eFPGA technology also enables so-called crypto agility, which is the ability to update underlaying cryptographic algorithms and protocols, even after an SoC/ASIC has already been deployed into the field.

QuickLogic's eFPGA IP is generated using the Australis IP generator, which supports any foundry and any process geometry while at the same time having the ability to create customized eFPGA IP that meets customers' PPA requirements and provides the ideal hardware platform for post-quantum cryptographic algorithms. Combining Xiphera's xQlave PQC solutions with traditional cryptographic algorithms (ECC or RSA) into a hybrid scheme enables a future-proof secure system on new and already existing eFPGA platforms.

"This partnership allows us to leverage the power of hardware acceleration and quantum-secure algorithms to deliver enhanced data protection and performance for our customers," said Mao Wang, senior director of product marketing at QuickLogic.

"With the rise of quantum computing, and government mandates to protect critical infrastructures against the threat posed by it, the time to address post-quantum cryptography in hardware security design is now. Xiphera's standards-based PQC IP combined with the design flexibility of QuickLogic's eFPGA platform enables solution designers to cost-effectively meet the rapidly evolving market demands for quantum-resilience," said Tommi Lampila, director of business development at Xiphera.

8.UK Security Agency Publishes New Crypto Designs

by Phil Muncaster
https://www.infosecurity-magazine.com/news/uk-security-agency-new-crypto/

The UK's National Cyber Security Centre (NCSC) looked to burnish its tech credentials this week with the publication of new research into robust cryptography.

The GCHQ offshoot is the UK national technical authority for cryptography, meaning it doesn't just produce guidance for government and business but also cutting-edge research.

The new paper from the NCSC's Peter Campbell presents two new designs which he hopes will "support the research that will inform the recently announced effort by NIST to standardize new modes of operation."

Named after the Latin names of two cities close to GCHQ headquarters, Glevian and Vigornian are new designs for the crypto algorithms known as "block cipher modes of operation," or "modes."

NCSC head of crypto research, John H, explained in a blog post yesterday (21 Sep 2023) that the new designs are intended to mitigate risk stemming from accidental misuse of crypto.

"The novelty in our research is a particular combination of strong robustness properties in the designs,

meaning that cryptographic security is maintained even in the event of significant human error in their deployment or use," he said.

"This robustness helps build assurance into the design and development of systems, in line with the principles of security by design and default, a key aim of modern cybersecurity practice."

He said the paper would help to inform NIST's efforts to standardize new, more robust modes.

The discoveries will have relevance to the commercial world, but not all organizations may find them cost-effective, John H added.

"In the NCSC, we design cryptography principally for use cases where long-term security is required, or where data has some sensitivity to it, so we take a very risk-averse approach to its handling," he continued.

"Of course not all cryptographers will make the same prioritization decisions as us in their designs. For example, we usually prefer to keep designs as simple as possible, even if that comes at some cost in performance."

9.Mastercard preps for the post-quantum cybersecurity threat

by Poornima Apte
https://www.cio.com/article/652972/mastercard-preps-for-the-post-quantum-cybersecurity-threat.html

The ecosystem of digital payments is a sitting duck.

The billions of transactions we conduct online today are protected by what are called public-key encryption technologies. But as quantum computers become more powerful, they will be able to break these cryptographic algorithms. Such a cryptographically relevant quantum computer (CRQC) could deliver a devastating impact to global cybersecurity protocols.

To prepare for this worst-case scenario, Mastercard launched its Quantum Security and Communications project, which earned the company a 2023 US CIO 100 Award for IT innovation and leadership.

"We're working proactively to mitigate the future risks related to quantum computing that could impact the security of the billions of digital transactions we process globally," says George Maddaloni, chief technology officer of operations at Mastercard, explaining the impetus for the project.

The post-quantum cybersecurity landscape

As it stands today, the online transactions that you and I conduct swear allegiance to public-key cryptography. In this technique, the person (or entity) sending the message secures (locks) it with a publicly available "key" and the entity at the receiving end decrypts it with a private key. The premise is that since only the receiver has the private key, the transaction is secure.

Secure private keys derive from mathematical algorithms — the Rivest-Shamir-Adleman (RSA) algorithm is a common one — that are impossible to reverse-engineer and hack. At least until a CQRC gets here

and does so through sheer brute force of quantum computing.

Entities in the private and public sector are preparing by following one of two tracks: working on a whole new set of quantum-resistant algorithms on which to base the private keys (post-quantum cryptography, PQC) or using quantum physics to do the same (quantum key distribution, QKD). Mastercard's project focuses on the latter method. Other enterprises in the financial sector are also exploring QKD.

On a parallel track, public institutions such as the National Institute of Standards and Commerce (NIST) are following the "harden-the algorithms" PQC approach. NIST has selected four quantum-resistant algorithms and is in the process of standardizing them. The final ones are expected to be available in the first half of 2024 and NIST has established a quantum-readiness roadmap for enterprises to follow.

The Mastercard project

Given that Mastercard has embraced the quantum key distribution method, its pilot project determined the architectural requirements and limitations of QKD and the operational readiness of the QKD systems.

Mastercard's Maddaloni reports that the team tested the quantum key distribution solution over a dark fiber network. Toshiba and ID Quantique were used to produce the keys. Two networking vendors that Mastercard has worked with in the past were also brought in. Their input from an IP Ethernet networking perspective helped, Maddaloni says. The goal was to conduct an inventory of the types of networking capabilities within Mastercard's network, which has thousands of endpoints connected with a few different telecommunications capabilities. "We wanted to look at whether the quantum key distribution capabilities work in that environment," Maddaloni says.

"The availability of QKD-enabled services and equipment is very specialized and currently quite limited," Maddaloni says. "Not many hardware vendors have features available that can integrate with the QKD systems." Designing the test was also challenging. QKD requires individual photons to arrive at precise times, and quantum states used for encryption can be easily disturbed by external factors such as noise, temperature changes, and vibration, among other factors.

"The project was designed to meet these challenges and deliver provable results and validation of the technology potential," Maddaloni adds. And it was successful.

The great migration

Questions of cybersecurity like the ones Mastercard is addressing are key because they address the very foundation of the system that financial institutions have built.

"Transaction security and the trust of our customers are the backbone of our business," Maddaloni points out. "The impact of current PKI encryption methods being compromised could quite literally threaten our ability to operate securely," he adds. "We believe being ready for a post-quantum landscape is part of our job and sends the right message to our partners, our customers, and our regulators."

Jeff Miller, CIO and senior vice president of IT and Security at Quantinuum, a full-stack quantum services company, agrees that protecting data is vital because "it's a conversation of trust with the consumer." The process of being crypto-agile is realizing that bad actors get more creative in the ways that they break into environments. As a result, enterprises must continue to build an iterative process and develop protocols to address these vulnerabilities.

While financial companies such as Mastercard are gearing up using their own pilot projects, the industry standards committee X9 is also working on guidance for enterprises in the financial sector, points out Dr. Dustin Moody, a mathematician who leads the post-quantum cryptography project at the National Institute of Standards and Technology (NIST).

The road ahead is not easy, the experts admit. “The availability of quantum key distribution services and equipment is still very limited. Some of the hardware vendors we worked with have features that are just announced and very new in the market, and some haven’t even been generally made available,” Maddaloni points out. “I do think that the industry understands that financial services will need this capability in the future.”

Moody advises companies to hone their post-quantum readiness despite what might look like a daunting landscape. The first order of business? “You need to find all instances of public-key cryptography, which is tricky and it will take time to do that inventory,” Moody says. “It’s gonna be a complex migration that will take time,” he says, “so we encourage organizations to get ahead of it as soon as they can.”

Miller agrees. He likens the process to preparing for Y2K, when enterprises were worried about formatting and storage of information beyond the year 2000. The migration to post-quantum preparedness even has a similar catchy acronym: Y2Q. A key difference, Miller says, is that there was a fixed countdown clock to Y2K. The cryptographically relevant quantum computer is not here today but it could be five years from now. Or ten.

“Knowing that we don’t have a firm date for when our current encryption methodologies are no longer useful,” Miller says, “that’s what keeps me awake at night.”

10.The Signal Protocol used by 1+ billion people is getting a post-quantum makeover

by Dan Goodin
https://arstechnica-com.cdn.ampproject.org/c/s/arstechnica.com/security/2023/09/signal-preps-its-encryption-engine-for-the-quantum-doomsday-inevitability/amp/

The Signal Foundation, maker of the Signal Protocol that encrypts messages sent by more than a billion people, has rolled out an update designed to prepare for a very real prospect that’s never far from the thoughts of just about every security engineer on the planet: the catastrophic fall of cryptographic protocols that secure some of the most sensitive secrets today.

The Signal Protocol is a key ingredient in the Signal, Google RCS, and WhatsApp messengers, which collectively have more than 1 billion users. It’s the engine that provides end-to-end encryption, meaning messages encrypted with the apps can be decrypted only by the recipients and no one else, including the platforms enabling the service. Until now, the Signal Protocol encrypted messages and voice calls with X3DH, a specification based on a form of cryptography known as Elliptic Curve Diffie-Hellman.

Safe... but for how much longer?

The one-way function for RSA works in a similar manner but relies on the multiplication and factorization of large prime numbers. It is computationally easy to multiply two large primes together to compute their product, but it's much more computationally intensive to find the original primes from their product.

Asymmetric cryptography is ideal for confidentiality on the Internet because it solves the challenge of

securely exchanging keys through an untrusted medium among two or more people who have never met. The robustness of these forms of encryption, however, breaks down in quantum computing. Under a concept known as superposition, the 0 and 1 binary bits found in classical computing are replaced with qubits, where 0s and 1s can in essence exist in multiple states at once.

A factorization method known as Shor's algorithm is widely believed to make it possible for a quantum computer with a sufficient number of qubits to break asymmetric encryption based on the difficulty of solving one-way functions. The current estimate is that to break RSA encryption with either 1,024 or 2,048 bits, it would take a quantum computer with about 20 million qubits running in superposition for about eight hours.

Currently, the largest quantum computer known to be in existence today runs with just 433 qubits. Estimates vary widely as to how long it will be until there's a large and robust enough quantum computer to break ECC and other vulnerable algorithms. Some expert forecasts predict as few as five years, while others say it could be 30 or more years out.

Enter PQC

There is little disagreement, however, that there will come a day when many of the most widely used forms of encryption will die at the hands of quantum computing. To head off that doomsday eventuality, engineers and mathematicians have been developing a new class of PQC, short for post-quantum cryptography.

The PQC added to the Signal Protocol on Monday is called PQXDH. It uses the same X3DH specification the Signal Protocol has always employed. On top, it adds an additional layer of encryption using Crystals-Kyber, one of four PQC algorithms the National Institute of Standards and Technology selected last year as a potential replacement to ECC and other quantum-vulnerable forms of encryption.

In a post published Tuesday (19 Sep 2023), Signal Foundation CTO Ehren Kret wrote:

> We believe that the key encapsulation mechanism we have selected, CRYSTALS-Kyber, is built on solid foundations, but to be safe we do not want to simply replace our existing elliptic curve cryptography foundations with a post-quantum public key cryptosystem. Instead, we are augmenting our existing cryptosystems such that an attacker must break *both* systems in order to compute the keys protecting people's communications.
>
> The essence of our protocol upgrade from X3DH to PQXDH is to compute a shared secret, data known only to the parties involved in a private communication session, using both the elliptic curve key agreement protocol X25519 and the post-quantum key encapsulation mechanism CRYSTALS-Kyber. We then combine these two shared secrets together so that any attacker must break both X25519 and CRYSTALS-Kyber to compute the same shared secret.

There's good reason for using both ECC and CRYSTALS-Kyber. Less than two months after NIST last year selected the four PQC algorithm candidate replacements, one of them was taken out of the running after researchers devised a technique that used complex mathematics and a single traditional PC to recover the encryption keys underlying the algorithm. The spectacular downfall of SIKE—as the PQC algorithm is known—underscores the risks inherent in the transition away from traditional forms of cryptography.

A PQC algorithm Google has proposed for the FIDO2 industry standard for logging in to websites takes a similar approach. It combines the Elliptic Curve Signature Algorithm with CRYSTALS-Dilithium, one of

the other three PQC algorithms still under consideration by NIST.

For now, the Signal app will use both the X3DH and the PQXDH. When all parties in a discussion have new versions of Signal installed, PQXDH will be used. When one or more of the parties are using older versions, conversations will be encrypted with X3DH. Eventually, Kret said he expects the Signal Protocol will use only the newer algorithm.

“We will need to make further upgrades to address the threat of an attacker with a contemporaneous quantum computer,” the CTO wrote. “Further research in the area of post-quantum cryptography will be needed to fill in the remaining gaps.”

11.QuickLogic and Xiphera Partner to Pioneer Post-Quantum Cryptography on eFPGAs

https://www.design-reuse.com/news/54839/quicklogic-xiphera-post-quantum-cryptography-efpga.html

Xiphera, a provider of hardware-based cryptographic security solutions, including Post-Quantum Cryptography (PQC) , today announced a partnership with QuickLogic Corporation, a developer of embedded FPGA (eFPGA) IP, ruggedized FPGAs and Endpoint AI/ML solutions, to implement Xiphera’s xQlave® quantum-secure cryptographic IP cores on QuickLogic's eFPGA architecture. This partnership provides architects with a path towards securing their assets against the quantum threat, enabling them to stay one step ahead in the evolving landscape of cyber threats.

With the rapid development of quantum computers and the increasing threat they pose to information and network security, the need for robust cybersecurity measures has become more crucial than ever. Xiphera answers the quantum-threat with its **xQlave® family of PQC IP cores**. The family includes **ML-KEM (Kyber)** and ML-DSA(Dilithium) – primary PQC algorithms in the PQC standard draft of the National Institute of Standards and Technology (NIST) – with logic-only implementations. Together, these IP cores provide quantum-secure key exchange, digital signature and authentication.

eFPGA technology offers two key benefits to implementing hardware security – distributed on-chip programmability, and the ability to parallelize intensive algorithmic computation requirements. This enables the eFPGA IP cores to offload heavy cryptographic operations from processor/software implementations, resulting in superior boot up and key calculation times. Furthermore, keys and secrets can be isolated from the rest of the system providing secure access only to trusted components. eFPGA technology also enables so-called crypto agility, which is the ability to update underlaying cryptographic algorithms and protocols, even after an SoC/ASIC has already been deployed into the field.

QuickLogic's **eFPGA IP** is generated using the Australis™ IP generator, which supports any foundry and any process geometry while at the same time having the ability to create customized eFPGA IP that meets customers’ PPA requirements and provides the ideal hardware platform for post-quantum cryptographic algorithms. Combining Xiphera’s xQlave™ PQC solutions with traditional cryptographic algorithms (ECC or RSA) into a hybrid scheme enables a future-proof secure system on new and already existing eFPGA platforms.

Benefits of the joint solution:

- **Data Protection:** Implementing xQlave® ML-KEM (Kyber) on QuickLogic's eFPGA architecture reinforces product security architecture, ensuring data protection against future threats.
- **Enhanced Performance:** Hardware acceleration through QuickLogic's eFPGA architecture significantly optimizes the performance of Xiphera's xQlave® family's ML-KEM (Kyber) and ML-DSA (Dilithium) IP cores.
- **Secure Storage:** The secluded block RAMs of the QuickLogic eFPGA architecture enable secure storage of secrets, without allowing privileged upper system components to access them.
- **Future Compatibility:** The implementation allows for easy upgrades to support the final NIST PQC standards when available, ensuring mission-critical systems remain secure against quantum threats.

"This partnership allows us to leverage the power of hardware acceleration and quantum-secure algorithms to deliver enhanced data protection and performance for our customers," said Mao Wang, senior director of product marketing at QuickLogic.

"With the rise of quantum computing, and government mandates to protect critical infrastructures against the threat posed by it, the time to address post-quantum cryptography in hardware security design is now. Xiphera's standards-based PQC IP combined with the design flexibility of QuickLogic's eFPGA platform enables solution designers to cost-effectively meet the rapidly evolving market demands for quantum-resilience," said Tommi Lampila, director of business development at Xiphera.

Availability

The QuickLogic and Xiphera solution for post-quantum cryptography is available now. Customers can contact Xiphera at info(at)xiphera.com or QuickLogic at info(at)quicklogic.com for more information.

Quantum computers are rapidly developing and pose a serious threat to the security of our current information and network infrastructures. This makes the need for robust cybersecurity measures more critical than ever.

NIST published Post-Quantum Cryptography (PQC) draft standards in 2023, a set of encryption algorithms that are resistant to attack by quantum computers. The NSA has also issued a requirement to implement quantum-secure algorithms in newly deployed systems by 2025, and to transition all deployed systems by 2030.

Flexibility and customization of eFPGAs make them the optimal choice for facilitating the migration of critical environments to quantum resilience with PQC.

12.Data Security in Blockchain with Cryptography

by LCX Team
https://www.lcx.com/data-security-in-blockchain-with-cryptography/

Cryptography is a method for protecting information from unauthorized access. Using cryptography, the blockchain secures transactions between nodes in the network. Blockchain is comprised of two key

concepts: cryptography and hashing. Cryptography encrypts messages in the P2P network, whereas hashing assists in securing block information and linking blocks in the blockchain. Cryptography focuses predominantly on ensuring the security of participants, transactions, and double-spending. It aids in securing various blockchain network transactions. It ensures that only the individuals for whom the transaction data is intended can access, read, and process the transaction data.

Enhancing Blockchain Security With Cryptography

Cryptography plays a pivotal role in enhancing the security of blockchain networks. Here are some ways in which cryptography safeguards the blockchain:

Data Integrity: Cryptographic hash functions ensure the integrity of data stored in the blockchain by generating unique hashes for each data block. Any tampering or alteration of data within the blockchain would result in a different hash value, immediately alerting the network to the presence of unauthorized changes.

Confidentiality: Encryption techniques, such as asymmetric encryption, can be employed to protect sensitive information within the blockchain. By encrypting data with the recipient's public key, only the intended recipient possessing the corresponding private key can decrypt and access the information. This ensures that sensitive data remains confidential even if stored on a public blockchain.

Authentication and Non-repudiation: Digital signatures allow participants in the blockchain network to verify the authenticity of transactions and messages. By digitally signing transactions using their private keys, participants can prove their identity and ensure non-repudiation, preventing any denial of involvement in the transaction.

Secure Key Management: Cryptography provides secure key management mechanisms that allow participants to generate, store, and distribute cryptographic keys securely. Robust key management practices ensure that keys remain protected from unauthorized access and can be reliably used for encryption, decryption, and digital signatures. Cryptography plays a pivotal role in enhancing the security of blockchain networks. Here are some ways in which cryptography safeguards the blockchain:

Cryptographic Components in Blockchain

A blockchain is a distributed ledger that records transactions across a network of computers. Cryptography forms the backbone of blockchain technology, ensuring the immutability, security, and trustworthiness of the data stored within the blockchain. Let's explore some key cryptographic components within the blockchain ecosystem:

Hash Functions: Hash functions are an integral part of blockchain technology. They take an input of any size and produce a fixed-length string of characters, known as the hash. Hash functions are designed to be one-way functions, meaning it is computationally infeasible to derive the original input from the generated hash. This property ensures the integrity of data stored on the blockchain.

Digital Signatures: Digital signatures are cryptographic mechanisms that provide authentication and non-repudiation within a blockchain. They use a combination of public and private key pairs to verify the authenticity of transactions. A digital signature is generated using the sender's private key, and it can be verified using the corresponding public key. This ensures that the message or transaction originated from the legitimate sender and has not been tampered with during transmission.

Symmetric and Asymmetric Encryption: Encryption plays a crucial role in securing sensitive data within the blockchain. Symmetric encryption uses a single shared key for both encryption and decryption processes, while asymmetric encryption uses a pair of mathematically related keys, namely the public

key and private key. Asymmetric encryption is commonly used for key distribution, establishing secure channels, and ensuring confidentiality within the blockchain network.

Merkle Trees: Merkle trees, also known as hash trees, are data structures used to efficiently verify the integrity and consistency of large sets of data stored in the blockchain. They employ hash functions to generate hash values for individual data blocks, which are then combined to form a hierarchical structure. Merkle trees allow for quick verification of specific data blocks without the need to traverse the entire blockchain, enhancing efficiency and security.

Conclusion

Cryptography lies at the core of blockchain technology, providing the essential security mechanisms necessary to establish trust and enable secure transactions in the digital age. By leveraging cryptographic techniques such as public-key cryptography, hash functions, and Merkle trees, blockchain systems offer enhanced security, transparency, and efficiency across a wide range of industries. As the adoption of blockchain technology continues to expand, understanding the symbiotic relationship between cryptography and blockchain becomes increasingly vital for businesses and individuals alike. Embracing this transformative power can unlock new opportunities, foster innovation, and shape the future of our interconnected world.

13.NIST Announces 2024 Timeline for First Standardized Post-Quantum Cryptography (PQC) Algorithms

by Casey Crane
https://www.thesslstore.com/blog/nist-announces-2024-timeline-for-first-standardized-post-quantum-cryptography-pqc-algorithms/

The U.S. federal standards body announced that three quantum-safe algorithms are expected to be ready for use next year. Now through Nov. 22, 2023, NIST is accepting feedback from the cryptographic community on those draft standards.

We've been talking about the need for post-quantum cryptography (PQC) now for a few years. As you can imagine, developing and rolling out new encryption standards for the entire internet takes a while. However, another significant milestone was recently achieved.

On Aug. 24, the National Institute of Standards and Technology (NIST) announced a public comments period for the first three Post Quantum Cryptography (PQC) algorithms' proposed standards drafts. These Federal Information Processing Standards (FIPS) aim to address the suspected dangers associated with cryptographically relevant quantum computer (CRQP) capabilities. The drafts of these algorithms, which were announced in July 2022, are open to comments through Nov. 22, 2023.

This public comment period allows members of the cryptographic community to share their thoughts, concerns, and recommendations relating to three cryptographic schemes. This way, changes or improvements can be made before the standards are ready for use in 2024.

So, what's the significance of all this to your organization and the industry as a whole?

What's the Significance of the 2024 Post-Quantum Cryptography Timeline?

These standards represent a big step toward data security in a post-quantum cryptography world. NIST anticipates that the standards will be available for use in 2024. The sooner NIST can standardize these FIPS, the faster public and private organizations can begin implementing quantum-safe algorithms within their environments. (But even after the standards are approved, it'll still take years or decades to make the full transition.)

In May 2022, the White House released its National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. The document states that the goal is to move "the maximum number of systems off quantum-vulnerable cryptography within a decade of the publication of the initial set of standards." There also will be a proposed timeline for deprecating quantum-vulnerable cryptographic standards.

We recently shared that Google announced the adoption of a hybrid PQC algorithm in the Chrome 116 version release of its browser. This is just one example of how industry leaders are starting to shift toward PQC-safe digital environments.

"PQC" Doesn't Convey the True Urgency of This Effort

Doesn't the term "post-quantum cryptography" mean that you don't need to have it in place until quantum computers are commercially available? NO. The name "post-quantum cryptography" is a bit of a misnomer. Experts within the industry use other names for post-quantum cryptography interchangeably: "quantum-resistant cryptography" and "quantum-safe cryptography."

Tim Hollebeek, Industry and Standards Technical Strategist at DigiCert, says he thinks quantum-safe cryptography is the most accurate. Hollebeek shared in a recent LinkedIn post that the PQC term gives people the wrong impression regarding the need or urgency for adoption:

> *"The problem with the term post-quantum cryptography is that it is easy to misunderstand as something you don't need to do until cryptographically relevant quantum computers (CRQCs) arrive, which that's the exact opposite of true. Quantum-safe cryptography is what you need to start using early enough so that ALL of your data and communications have been COMPLETELY migrated before the EARLIEST possible date when Dr. Evil will have access to his pet CRQCodile-9000. And remember, he won't publicly announce it!"*

Translation: Although quantum computers that can break modern encryption schemes don't currently exist, it doesn't mean that your organization shouldn't be planning or starting to prepare for this eventual reality now. And part of that planning should include how you'll securely manage your cryptographic keys' lifecycles.

It doesn't matter whether the emergence of quantum computing happens in two years or 20: start getting your ducks in a row now, so you won't be caught off guard later.

An Overview of the Three Proposed Algorithms

In its July 2022 PQC algorithm selection announcement, NIST selected four candidate algorithms as the finalists. NIST has opened public comments for three of those four standards (FIPS 203, 204, and 205) now, and announced that it will release the draft standards of the fourth (FALCON) for public comments in 2024.

So, what are these standards? We've talked about them before, but let's quickly review what they are and how they're intended to be used.

1. **FIPS 203.** This module lattice-based key encapsulation mechanism (ML-KEM), based on CRYSTALS-Kyber**,** is used to establish a shared secret key over open (i.e., insecure) channels. Think of this as the replacement for factor-based key agreement schemes for public-facing environments (e.g., RSA), which are expected to be broken by quantum computing. An example of this type of application would be securing connections for websites and web apps.

2. **FIPS 204.** The modern lattice-based digital signature algorithm (ML-DSA) consists of three algorithms for generating cryptographic keys, digital signing, and verifying the resulting digital signature and is based on CRYSTALS-Dilithium. An example of where this could be used is for remote document signing.

3. **FIPS 205.** The stateless hash-based digital signature algorithm (SLH-DSA) is a cryptographic function that aims to reduce signature sizes. It's based on SPHINCS+ and operates differently from the other algorithms at a mathematical level. Much like CRYSTALS-Dilithium, this algorithm would be best suited for remote digital signing.

To learn more about each of these algorithms and their FIPS proposed standards, click on the links listed above.

Let's Wrap This Up

Quantum-related threats are coming; it's a matter of *when*, not *if*. To prepare for this, you can adopt a hybrid approach:

- **Use modern strong cryptographic algorithms within your environment**. This will help to protect your data against current threats.

- **Incorporate new, quantum-safe algorithms as they become available.** This will help protect your current data against future threats (i.e., "harvest now, decrypt later" [HNDL] attacks). The concern is that bad guys will steal your sensitive info now and sit on it until CRQC capabilities are available, and use it to decrypt evergreen data (IP, personally identifiable information that have long lifespans [such as social security numbers, birthdates, etc.]).

- **Implement and automate secure key management.** After all, cryptographic algorithms won't do you any good if you don't properly secure the keys they rely on.

Quantum computers will, inevitably, be a part of our lives in the future. So, while it's important not to panic, it's even more important to start planning and making your preparations now.

14.Why It's Time to Implement a Quantum Safe Network

by Grégoire Ribordy
https://www.forbes.com/sites/forbesbusinesscouncil/2023/09/14/why-its-time-to-implement-a-quantum-safe-network/?sh=26c357cb27f7

Like AI, quantum computing has been met with mixed feelings.

A quantum computer's ability to exponentially speed up certain tasks and to solve problems that are mathematically challenging for classical computers means it could revolutionize the fields of materials science, pharmaceutical research, investment, supply chain management and even machine learning that rely upon calculation and simulation.

This computational power does, however, pose a fundamental threat to the public key infrastructure the world relies on for cybersecurity. Cracking the cryptographic systems in place today is difficult because the math is hard—problems that can be solved by a quantum computer in a matter of hours, minutes or seconds would take the most powerful of today's classical computers hundreds, if not thousands, of years.

Act Today to Secure The Future

Conventional wisdom states we are in the quantum decade. By the end of the 2020s, there will be commercially viable quantum computing resources widely available.

Much of the data that traverses today's public and private network infrastructure is sensitive in nature—private citizen data, national security, financial records, healthcare data, intellectual property. This exposes it to "harvest now, decrypt later" attacks. To secure today's infrastructure for tomorrow, there are two separate—but complementary—solutions available:

- Post-quantum cryptography (PQC) is the use of next-generation crypto algorithms that are believed to be resistant to quantum cyberattacks.
- Quantum key distribution (QKD) is a secure platform that provides guaranteed forward secrecy of encryption keys.

Together, they address the core cryptographic principles of confidentiality, integrity, authenticity, non-repudiation and key management.

Post Quantum Cryptography

In the U.S., the National Institute of Standards and Technology (NIST) has been working to develop the first set of standardized post-quantum algorithms since 2016. The first Federal Information Processing Standard (FIPS) for PQC is expected in 2024.

Theoretically, the migration from classical to post-quantum algorithms should be simple. However, the reality will likely be somewhat different. Some existing cryptographic systems lack the agility required to "hot swap" algorithms or to add plug-and-play PQC, which may require wholesale replacement. Other incumbent systems may struggle with the computing power and data rates associated with PQC.

Despite these potential limitations, some solutions on the market offer hybrid encryption, a mix of classical Advanced Encryption Standard- and NIST-shortlisted algorithms.

There are still some security concerns over these new algorithms. Some of the candidate algorithms have been compromised using classical computing methods. The longer-term security of PQC is also yet to be proven. We only know that quantum-resilient technology today is not vulnerable to currently known quantum algorithms. As quantum technology evolves, alternative algorithms will emerge.

Quantum Key Distribution

QKD provides additional security to network infrastructure, independent of computational power. Importantly, it offers a future-proof solution. QKD leverages the fundamental principles of quantum mechanics to guarantee forward secrecy of encryption keys.

QKD is a much more mature technology than PQC, with players from all around the world, including my company, ID Quantique, in Switzerland, as well as QuantumCTek in China, Qubitekk in the U.S., Toshiba in Japan and many new start-ups financed by record 2022 investments.

QKD is not a standalone technology. As a key exchange mechanism, it still requires authentication and is used in conjunction with VPNs or encryptors to provide quantum-safe security across network infrastructure at rates of up to 100Gbps.

Originally used to secure point-to-point networks, scalable QKD infrastructure is now in development, with trusted nodes and key management systems being employed to extend the range and topology of secure networks.

Criticism of the technology has centered around its effective range, but developers have successfully extended the transmission distance of QKD to over 800 kilometers across optical fibers in recent years, and the use of QKD in free space (using low orbit satellite relays) as well as a mesh network setup is eliminating geographical barriers.

The Best of Both Worlds

The next generation of secure networks will likely need to feature both PQC and QKD. The public key infrastructure we rely on to secure the internet will transition to incorporate newly standardized PQC algorithms. At first, these will operate in a hybrid mode, alongside today's ECC and RSA algorithms, until the classical security of PQC is proven.

Where long-term confidentiality, high-assurance security and high-density data are needed, local and regional QKD infrastructure could be used to ensure data protection. The security of any system is only as good as its weakest link. In a hybrid infrastructure—where QKD sits at the core of the network and PQC extends security to the edge—the attack surface should be significantly reduced.

This enhances the overall security of the network and enables the introduction of zero-trust architecture. For cloud and telecommunications service providers, this provides a point of differentiation that will appeal to customers seeking "secure by design" solutions.

An Evolving Ecosystem

Quantum technologies are undergoing rapid expansion. Alongside the evolution of PQC and QKD technologies, progress in quantum memory and quantum repeaters is creating the foundation for a quantum internet.

Scalability, agility and availability of secure key exchange are facilitated through specific key management systems. Software plays a critical role in maintaining tomorrow's end-to-end, quantum-safe infrastructure. It enables the extension of QKD networks beyond simple point-to-point architecture and acts as the catalyst that ensures long-distance key distribution throughout complex network topologies. Used in combination with PQC, it maintains a coherent security ecosystem.

A major contributor to the adoption of QKD is its current progress in standardization. Industry players must continue working together to define the standardization and certification wireframes. Every new step brings greater trust in quantum technologies. Standards play a central role in building trust, as the agreement of standards is a sign of the maturity of a technology and its supporting ecosystem.

Before the end of the decade, we should see quantum computing, communications and networking working hand in hand with classical technologies to deliver next-generation security, confidentiality, authenticity and integrity of data. The technology is already being implemented around the world to secure

key networks requiring long-term security. It's time to act now to reach this point of safety.

15.QuSecure's Quantum-Resilient SaaS is Industry's First and Only Post-Quantum Cryptography Solution Now Available via GSA Multiple Award Schedule

by Dan Spalding
https://www.businesswire.com/news/home/20230914758932/en/QuSecure%E2%80%99s-Quantum-Resilient-SaaS-is-Industry%E2%80%99s-First-and-Only-Post-Quantum-Cryptography-Solution-Now-Available-via-GSA-Multiple-Award-Schedule

QuSecure™, Inc., a leader in post-quantum cryptography (PQC), today announced that its state-of-the-art PQC products are now available through the General Services Administration (GSA) Multiple Award Schedule (MAS). This strategic move enhances QuSecure's commitment to delivering advanced cybersecurity technologies to federal government agencies and the broader public sector, ensuring data protection against the emerging threats of AI (Artificial Intelligence) and quantum computing. Being on the GSA schedule offers many significant benefits, including:

- **Direct Access to the World's Largest Customer** – The GSA Schedule enables direct access to the U.S. federal government, the largest buyer of goods and services in the world, and it allows QuSecure to more easily equip state and local governments, as well as public schools, with leading PQC technologies.
- **Access to GSA Schedule Opportunities** – QuSecure has access to opportunities that are available only to GSA Schedule contractors and these have the benefit of faster award times.
- **Competitive Advantage** – Government agencies often prefer to buy from the GSA Schedule program because the contractors such as QuSecure are pre-vetted and offer the best value.
- **Long-term Partnership** – GSA Schedule contracts with QuSecure can last up to 20 years and there is no ceiling on sales (also called "Indefinite Delivery, Indefinite Quantity").
- **Streamlined Procurement Process** – The GSA Schedule simplifies the procurement process for both the government buyer and QuSecure. A GSA Schedule contract is deemed a Governmentwide Acquisition Contract (GWAC) with "fair and reasonable pricing" and can be used by any federal entity. An order placed with QuSecure against a GSA Schedule contract automatically is considered the best value and results in the lowest overall cost for the customer.

QuSecure's quantum-resilient solutions are engineered to safeguard sensitive information against today's attacks and in the coming age of quantum computing, offering unparalleled security for government organizations and the public sector. With AI, ML (Machine Learning) and quantum computing's rapid advancements able to render current encryption methods obsolete, QuSecure stands at the forefront of delivering quantum-resilient cybersecurity.

Commenting on this significant development, Pete "Shadow" Ford, QuSecure EVP of Government Operations, stated, "As the quantum computing era continues to advance rapidly, data security has never been more critical for government agencies and public sector organizations. We are thrilled to offer our quantum-resilient PQC solutions through the GSA Schedule, further empowering these entities to secure their data and communications effectively."

Key benefits of QuSecure's products for the government and public sector include:

1. **Unmatched Quantum-Resistant Protection:** QuSecure's solutions use post-quantum cryptographic algorithms that are designed to withstand the computational power of quantum computers. This means that classified information, personal data, and critical infrastructure remain secure, even in the face of quantum threats. Additionally, QuSecure uniquely offers cryptographic agility which enables customers to change cryptography and key sizes with the click of a button.

2. **Compliance with Government Standards:** QuSecure's products adhere to stringent government security standards and certifications providing assurance that they meet the highest security requirements mandated by government agencies. In addition, QuSecure standardized its system with all the National Institute of Standards and Technology (NIST) finalist algorithms which, when combined with cryptographic agility, means that customers have flexibility to utilize any of the approved algorithms and key strengths.

3. **Seamless Integration:** QuSecure's solutions are designed for easy integration into existing government IT infrastructure, minimizing disruption while maximizing security. By using QuSecure, customers leave their existing encryption in place. This means that they can use QuSecure PQC in addition to their current encryption – minimizing risk, cost, and deployment time.

4. **Cost-Efficiency:** By adopting QuSecure's quantum-resilient solutions, government agencies can proactively protect their data and greatly minimize the likelihood of costly consequences of data breaches or security vulnerabilities exposed by quantum computing.

16.When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret

by Edward Parker
https://www.lawfaremedia.org/article/when-a-quantum-computer-is-able-to-break-our-encryption-it-won-t-be-a-secret

Quantum computers may eventually have devastating impacts on cybersecurity—but we'll probably see the threat coming in time to set up counters.

On Oct. 23, 2019, Google published a groundbreaking scientific research article announcing one of the "holy grails" of quantum computing research: For the first time ever, a quantum computer had solved a mathematical problem faster than the world's fastest supercomputer. In order to maximize impact, the Google team had kept the article tightly under wraps in the lead-up to publication—unusually, they had not posted a preprint to the arXiv preprint server.The article sank with barely a ripple in the expert academic community.

That wasn't because anyone disputed the significance of the Google team's milestone. Many experts still consider Google's demonstration to be the most important milestone in the history of quantum computing, comparable to the Wright brothers' first flight in 1903. But most experts in the field had already read the article. A month earlier, a NASA employee who was involved with the research had accidentally posted a draft of the article on NASA's public web site. It was online for only a few hours before being taken back down, but that was long enough. Schrödinger's cat was out of the bag.

This anecdote illustrates a fact with important policy implications: It is very difficult to keep groundbreaking progress in quantum computing secret.

One of the most important quantum computing algorithms, known as Shor's algorithm, would allow a large-scale quantum computer to quickly break essentially all of the encryption systems that are currently used to secure internet traffic against interception. Today's quantum computers are nowhere near large enough to execute Shor's algorithm in a practical setting, and the expert consensus is that these cryptanalytically relevant quantum computers (CRQCs) will not be developed until at least the 2030s.

Although the threat is not yet imminent, the consequences of a hostile actor's execution of Shor's algorithm could be incredibly dire. Encryption is at the very bedrock of most cybersecurity measures. A hostile actor who could read encrypted information transmitted over the internet would gain access to an immeasurable amount of critically sensitive information—from personal information such as medical or criminal records, to financial information such as bank account and credit card numbers, to cutting-edge commercial research and development, to classified national security information. The U.S. National Security Agency has said that "the impact of adversarial use of a quantum computer could be devastating to [National Security Systems] and our nation."

Fortunately, preemptive countermeasures are already being put into place. The U.S. National Institute of Standards and Technology (NIST) is standardizing new post-quantum cryptography (PQC) protocols that are expected to resist attacks from both standard and quantum computers. Upgrading communications systems to use post-quantum cryptography will be a long, complicated, and expensive process that will extend over many years. The U.S. government has already begun the process: In May 2022, President Biden issued National Security Memorandum 10, which gives directives to all U.S. government agencies regarding the U.S. government's transition to post-quantum cryptography. Recognizing the long timelines that this transition will require, the memorandum sets "the goal of mitigating as much of the quantum risk as is feasible by 2035.

Several experts have stated that one of the most important factors that will determine the severity of the threat posed by a CRQC is whether or not the public knows of the CRQC's existence. As soon as the existence of the CRQC becomes public knowledge—or is even considered plausible—and the threat becomes concrete, most vulnerable organizations will immediately move to upgrade all their communications systems to post-quantum cryptography. This forced transition may well be very expensive, chaotic, and disruptive, but it will fairly quickly neutralize most attack vectors (with one important exception mentioned below). The true nightmare scenario would be if a hostile actor (such as a criminal or terrorist organization or a hostile foreign government) *covertly* operated a CRQC over a long time period before PQC becomes universal, allowing the actor to collect a huge amount of sensitive information undetected.

Fortunately, it is extremely unlikely that any organization will develop a CRQC in secret, for at least four interrelated reasons.

First, anyone trying to develop a high-performance quantum computer will face stiff competition from commercial industry. Quantum computers have the potential to enable many commercial applications that have nothing to do with decryption, such as drug design, materials science, and numerical optimization. While there is huge uncertainty in the pace of technology development and the

timelines for useful applications, some people have predicted that quantum computers could deliver over a trillion dollars in economic value over the next decade. Many private companies are racing to produce state-of-the-art quantum computers in order to profit from these applications, and there is currently no clear technical industry leader. Moreover, these companies are collectively extremely well funded: U.S. quantum computing startups alone have raised over $1.2 billion in venture capital, and that total does not include other major players such as national laboratories, large self-funding companies, or non-U.S. companies.

In the near term, these companies face some incentives to publicize their technical capabilities and other incentives to keep them proprietary. But in the long run, companies need to advertise their capabilities at a reasonable level of technical detail in order to attract customers. The closer the state of the art in commercial industry comes to the technical performance required to execute Shor's algorithm, the clearer the threat will become to potential targets, and the more urgently they will prioritize upgrading to PQC.

Any organization attempting to secretly develop a CRQC would therefore need enormous financial resources in order to compete with the well-funded and competitive commercial industry, and it would need to stay *far* ahead of that industry in order to keep the element of surprise.

The second reason that a CRQC is unlikely to be developed in secret is that a relatively small number of people are at the cutting edge of quantum computing development in industry or academia, and they are well known within the expert community. Any organization attempting to secretly develop a CRQC would need to acquire world-class talent—and if many of the greatest technical experts suddenly left their organizations or stopped publishing in the technical literature, then that fact would immediately be fairly evident, just as it was during the Manhattan Project. (However, this point may become less relevant in the future as the commercial industry matures. As the pool of expert talent grows and more information becomes business proprietary, public information about the top technical talent may decrease.)

Third, a CRQC might be physically difficult to hide. It's extremely difficult to estimate the physical resources that will be required to operate a CRQC, but my recent research suggests that a CRQC might plausibly draw 125 megawatts of electrical power, which is a significant fraction of the total power produced by a typical coal-fired power plant. A device that requires its own dedicated power plant would leave considerable evidence of its existence. Certain very capable organizations (such as national governments) might be able to conceal such a project, but doing so would not be easy and could well be impossible for smaller organizations.

The fourth reason has to do with the relative resources required for various quantum computing applications. As with most technical questions regarding the future of quantum computers, there is a huge amount of uncertainty here. But there is fairly strong theoretical evidence that many commercial applications of quantum computers will be significantly technically easier to implement than Shor's algorithm. There is already very active research into the question of whether even today's crude quantum computers, known as noisy intermediate-scale quantum computers, might be able to deliver practical applications in the near future, although we don't yet know for sure.

In a more conservative technical scenario, all useful quantum applications might require a technically challenging hardware stabilization process known as quantum error correction, which has very high hardware requirements. But even in this scenario, there is evidence that some commercial applications of quantum computers (like the scientific modeling of chemical catalysis) will require lower hardware resources than Shor's algorithm does. For example, one recent analysis estimated that computationally modeling a chemical catalyst used for direct air carbon capture would require only 20 percent as many qubits as executing Shor's algorithm would. (A qubit is the basic building block of a quantum computer and one of the simplest ways to quantify its hardware performance.)

These analyses imply that commercial applications of quantum computing will very likely become technically feasible before decryption does. Unless an organization attempting to develop a CRQC is far more technically advanced than the commercial sector—which is unlikely, given the potentially huge economic value mentioned above—commercial companies will probably beat the organization to applications, and they will announce their success. Even in the unlikely event that an organization does manage to develop a CRQC before the commercial industry develops a commercially useful quantum computer, that organization will face an enormously high opportunity cost of *not* using its CRQC for commercial applications that could deliver billions of dollars of value. Even if the organization were government sponsored, its government sponsor would face an enormous economic incentive to use its quantum computer for commercial applications rather than for intelligence collection.

What this means for policymakers is that the ultimate worst-case scenario, in which a hostile actor secretly deploys a CRQC for many years against totally unsuspecting victims, is highly unlikely. This does not in any way lessen the importance of quickly upgrading all critical communications systems to post-quantum cryptography, however, since doing so defends against harvest-now-decrypt-later attacks, in which a CRQC is deployed retroactively against saved encrypted data that was intercepted previously.

Operators of communications systems that transmit highly sensitive information should already be preparing to upgrade those systems' cryptography to PQC, and they should perhaps develop contingency plans for even further accelerating that adoption if signs arise that CRQCs are approaching unexpectedly quickly. But policymakers should also understand that the commercial applications of quantum computers will probably emerge well before intelligence-collection applications do. This conclusion may carry implications regarding appropriate national-security-related policies such as export controls and outbound investment restrictions, as well as the broader balance of risks and benefits around quantum computers.

Finally, policymakers and cybersecurity analysts should avoid messaging that emphasizes the risk that CRQCs developed in secret could be imminent or already operational (unless, of course, they have additional information that runs counter to the points raised above). There is already more than enough reason to upgrade our communications systems to resist attacks from quantum computers as soon as possible. Even if completely unexpected attacks from a black-swan quantum computer are unlikely, attacks from known or suspected quantum computers would already be plenty bad enough.

17.UAE unveils world's first open-source software library for cryptographic estimations

by Staff Writer
https://www.edgemiddleeast.com/emergent-tech/uae-unveils-worlds-first-open-source-software-library-for-cryptographic-estimations

With the advent of quantum computing on the horizon, traditional cryptographic methods are facing an existential threat. In response to this challenge, UAE's Technology Innovation Institute's (TII), Cryptography Research Center (CRC) has taken a monumental step forward by unveiling the CryptographicEstimators, the world's first open-source software library entirely dedicated to assessing the security of Post-Quantum Cryptography (PQC) schemes.

The challenge of Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) is the new frontier in securing digital communication. As quantum computers become more powerful, traditional cryptographic systems that have been the bedrock of online security for decades are at risk of being compromised. PQC aims to develop cryptographic methods that are resistant to quantum attacks, ensuring the continued safety of sensitive data and communications in a post-quantum world.

Assessing the security of PQC schemes is a complex and critical task. However, until now, cryptographic estimations have often been performed in an ad-hoc manner. This approach has led to the creation of non-standardised estimation scripts that produce inconsistent results when applied to the same cryptographic problems. Such inconsistencies present a significant obstacle to achieving a consensus on the security of cryptographic systems.

CryptographicEstimators: A game-changer in PQC security assessment

CryptographicEstimators is an open-source software library that provides a standardised platform for estimating the security of PQC schemes, including key exchange methods, public key encryption, and digital signatures.

Key features of CryptographicEstimators

1. **Consolidating Existing Estimators:** CryptographicEstimators consolidates existing estimation methods, ensuring that cryptographic assessments are carried out consistently and reliably.

2. **Foundation for New Estimators:** It serves as the foundation for the development of new estimation methods, fostering innovation in the field of PQC security assessment.

3. **Supporting Scheme Design and Evaluation:** This tool assists public key scheme designers in selecting secure parameters and empowers cryptanalysts to rigorously evaluate their findings against established benchmarks.

4. **Comprehensive Coverage:** Unlike similar projects that focus on single classes of hardness assumptions, CryptographicEstimators encompasses a wide spectrum of post-quantum secure foundations, making it a versatile and comprehensive resource.

The introduction of CryptographicEstimators is a pivotal moment in the world of cryptography. As the American National Institute of Standards and Technology (NIST) continues its efforts to standardise PQC, CryptographicEstimators emerges as a unique, state-of-the-art cryptographic tool. It positions TII as a global leader in the PQC domain and solidifies the UAE's role as a significant stakeholder in advancing the PQC ecosystem.

CryptographicEstimators not only complements TII's existing initiatives in cryptography but also contributes to the global mission of safeguarding digital communication in the face of quantum threats. It reinforces the importance of collaborative research and innovation in securing our digital future.

18.It's the end of the line for outdated internet encryption protocols

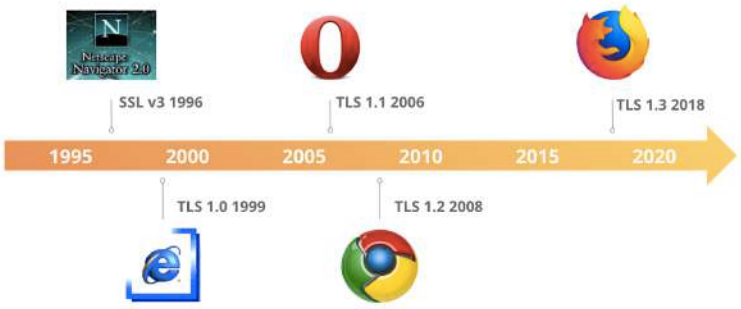
by David Strom
https://siliconangle.com/2023/09/11/end-line-outdated-internet-encryption-protocols/

An ageing core internet protocol is finally getting the ax by Microsoft Corp.

But it wasn't just last month's announcement that the software vendor was ending support for versions 1.0 and 1.1 of Transport Layer Security, or TLS, but that it was actually dropping the support from the impending release of the latest beta version of Windows 11.

TLS is one of those protocols that have far-reaching influence. It provides the security for encrypting web pages — designated with the "s" in HTTPS URLs for example. It also provides for encrypted connections used today in communications tools such as virtual private networks and secure command consoles called Secure Sockets Layer shells that operate numerous servers.

These protocol updates take time to develop, because they rely on a consensus approach with one of the internet's international standards bodies. The latest version of TLS is 1.3, which was adopted in the summer of 2018, replacing version 1.2 which came out in 2008 and 1.0 which was released in 1999.



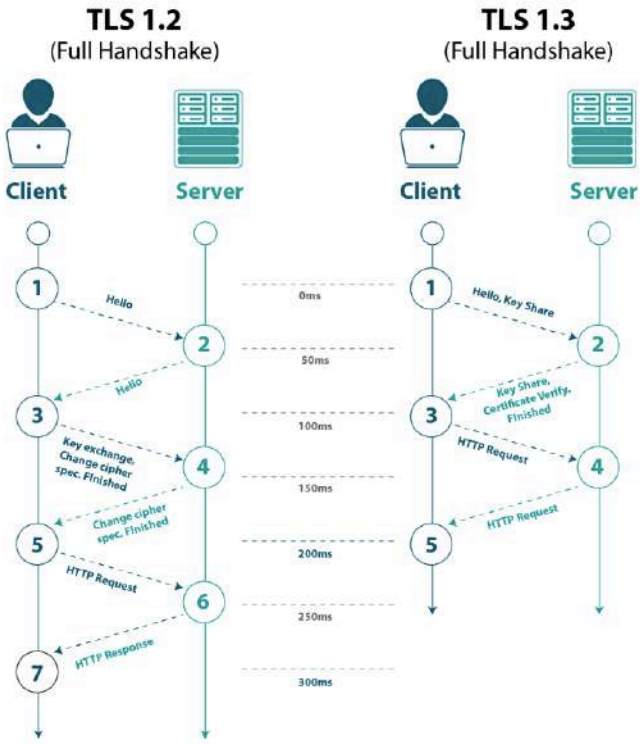
In the case of TLS 1.3, the process took five years from concept to implementation. Now most web traffic happens over HTTPS connections and we don't give this much thought. The new version speeded up network conversations by reducing overall latency – version 1.2 required two round trips, while 1.3 needs only at most a single round trip — and made the "handshakes" between two computers a lot more secure, as illustrated in the accompanying diagram.

But just reducing latency wasn't enough, and the older TLS version were vulnerable to attacks that were well-known and often used as initial exploits to penetrate networks, notoriously including 2014's Heartbleed attacks for example.

Cloudflare summarized five of these vulnerabilities in their blog post several years ago, basically identifying the progress in improving encryption keys. The latest TLS 1.3 version "make it impossible for someone to enable the vulnerable aspects of TLS 1.2," as they wrote in their blog, and this is why version 1.3 removed many legacy features.

The U.S. National Security Agency warned about these vulnerabilities back in 2021 and recommended

that organizations block all use of TLS 1.0 and 1.1. Most of the major web browser vendors have dropped their support for these versions for several years. Microsoft said in its announcement that "we have been tracking TLS protocol usage for several years and believe TLS 1.0 and TLS 1.1 usage data are low enough to act."



Nevertheless, there are still some places they are being used. The NSA warned, "Using obsolete encryption provides a false sense of security because it may look like sensitive data is protected, even though it really is not." That is excellent advice.

Significance of Microsoft's move

Microsoft said it will disable support of TLS 1.0 and 1.1 by default in the new Insider preview build of Windows 11 that's expected any day now and then in subsequent versions. But this doesn't mean Windows can't work with these aging protocols: Information technology administrators can turn this on with edits to the Windows Registry. That is somewhat time-consuming and painful, to be sure, and easily prone to mistakes.

Microsoft acknowledged the older protocol versions might still be used by a variety of applications, such as in ancient versions of its SQL Server and pre-2018 Intuit Turbo Tax versions. They assembled a series of suggestions to customers who may have problems with removing other dependencies in this document posted with revisions last month, and summarized the support of the various versions across its older Windows operating systems in the accompanying table.

How to find and fix obsolete systems

There have been numerous tools to help IT managers find and fix outdated TLS implementations. And

even though Microsoft is still supporting TLS 1.2, it is probably a good idea to update these deployments to version 1.3, because eventually Windows will move on to that protocol too.

Figure 1: Security Protocol Support by OS Version

Windows OS	SSLv2	SSLv3	TLS 1.0	TLS 1.1	TLS 1.2
Windows Vista	Enabled	Enabled	**Default**	Not Supported	Not Supported
Windows Server 2008	Enabled	Enabled	**Default**	Disabled*	Disabled*
Windows 7 (WS2008 R2)	Enabled	Enabled	**Default**	Disabled*	Disabled*
Windows 8 (WS2012)	Disabled	Enabled	Enabled	Enabled	**Default**
Windows 8.1 (WS2012 R2)	Disabled	Enabled	Enabled	Enabled	**Default**
Windows 10	Disabled	Enabled	Enabled	Enabled	**Default**
Windows Server 2016	Not Supported	Disabled	Enabled	Enabled	**Default**

*TLS 1.1/1.2 can be enabled on Windows Server 2008 via this optional Windows Update package.

The NSA has a collection of mitigation tools and best practice suggestions including Snort signatures to locate old TLS versions, templates for web server configurations and various network scanners. These are open source and free. One of those tools is from Qualys' SSL Labs that can test both browsers and server implementations of TLS.

TLS isn't the only upgrade target for Microsoft's cleanup campaign as of late. Last week (First week of September), it announced the end of support for legacy third-party printer device drivers, a decision that will take several years to trickle down through the various Windows products. These drivers were another source of potential vulnerabilities, as this post from Sentinel Labs wrote about in 2021.

19.New quantum random number generator could revolutionize encryption

by Help Net Security
https://www.helpnetsecurity.com/2023/09/08/random-number-generator-encryption/

Digital information exchange can be safer, cheaper and more environmentally friendly with the help of a new type of random number generator for encryption developed at Linköping University.

The researchers behind the study believe that the new technology paves the way for a new type of quantum communication.

Safeguarding data made simple with encryption

The most common way to protect information is through encryption. So when we send emails, pay bills and shop online, the information is digitally encrypted.

To encrypt information, a random number generator is used, which can either be a computer programme or the hardware itself. The random number generator provides keys that are used to both encrypt and unlock the information at the receiving end.

Different types of random number generators provide different levels of randomness and thus

security. Hardware is the much safer option as randomness is controlled by physical processes. And the hardware method that provides the best randomness is based on quantum phenomena – what researchers call the Quantum Random Number Generator, QRNG.

“In cryptography, it’s not only important that the numbers are random, but that you’re the only one who knows about them. With QRNG’s, we can certify that a large amount of the generated bits is private and thus completely secure. And if the laws of quantum physics are true, it should be impossible to eavesdrop without the recipient finding out,” says Guilherme B Xavier, researcher at the Department of Electrical Engineering at Linköping University.

His research group, together with researchers at the Department of Physics, Chemistry and Biology (IFM), has developed a new type of QRNG, that can be used for encryption, but also for betting and computer simulations. The new feature of the Linköping researchers’ QRNG is the use of light emitting diodes made from the crystal-like material perovskite.

Their random number generator is among the best produced and compares well with similar products. Thanks to the properties of perovskites, it has the potential to be cheaper and more environmentally friendly.

Optical instruments enter a new era

Feng Gao is a professor at IFM and has been researching perovskites for over a decade. He believes that the recent development of perovskite light emitting diodes (PeLEDs) means that there is an opportunity to revolutionise, for example, optical instruments.

“It’s possible to use, for example, a traditional laser for QRNG, but it’s expensive. If the technology is eventually to find its way into consumer electronics, it’s important that the cost is kept down and that the production is as environmentally friendly as possible. In addition, PeLEDs don’t require as much energy to run,” says Feng Gao.

The next step is to develop the material further to make the perovskite lead-free and to extend its lifetime, which is currently 22 days. According to Guilherme B Xavier, their new QRNG could be available for use in cybersecurity within five years.

“It’s an advantage if electronic components that are to be used for sensitive data are manufactured in Sweden. If you buy a complete randomness generator kit from another country, you can’t be sure that it’s not being monitored.”

20.North Korean hackers target security researchers with zero-day exploit

by Helga Labus
https://www.helpnetsecurity.com/2023/09/08/security-researchers-zero-day-compromise/

North Korean threat actors are once again attempting to compromise security researchers’ machines by employing a zero-day exploit.

The warning comes from Google’s own security researchers Clement Lecigne and Maddie Stone, who detailed the latest campaign mounted by government-backed attackers.

Security researchers targeted with zero-day

The attackers initially contacted the researchers through social media (e.g., X, formerly Twitter, or Mastodon) on the pretense of collaborating on security research. After they moved the conversation to end-to-end ecnrypted IM apps (Signal, WhatsApp or Wire) and established trust, they would deliver a malicious file containing a zero-day exploit.

“Upon successful exploitation, the shellcode conducts a series of anti-virtual machine checks and then sends the collected information, along with a screenshot, back to an attacker-controlled command and control domain,” Lecigne and Stone said.

The attackers also tried another trick: they pointed the researchers towards a Windows tool (GetSymbol) that downloads debugging symbols from Microsoft, Google, Mozilla and Citrix symbol servers for reverse engineers, but is also capable of downloading and executing arbitrary code from an attacker-controlled domain.

“If you have downloaded or run this tool, [Google] TAG recommends taking precautions to ensure your system is in a known clean state, likely requiring a reinstall of the operating system,” the researchers advised.

Google has yet to reveale which software is affected by the exploited the zero-day.

“The vulnerability has been reported to the affected vendor and is in the process of being patched. Once patched, we will release additional technical details and analysis of the exploits involved in line with our disclosure policies,” they added.

A new campaign

A similar campaign was revealed in January 2021, when threat actors, believed to be backed by the North Korean government, created accounts on Twitter, LinkedIn, Keybase, and Telegram to directly contact security researchers. (Microsoft also detailed that campaign.)

After establishing trust, they shared a link, asking the researchers to check the content. This would prompt the installation of a malicious service and a backdoor beaconing to a threat actor’s C2 server.

21.HSBC takes a deep dive into quantum computing

by Michela Menting
https://www.spiceworks.com/it-security/security-general/guest-article/post-quantum-cryptography-first-draft-standards-by-nist/

HSBC is collaborating with Terra Quantum on an experiment to test the use of quantum technology for optimising capital allocation.

The two firms have been exploring use cases for the technology in collateral management, using high grade mathematical and algorithmic strategies to balance risks, liquidity, and profitability.

Existing methods for collateral optimiation primarily rely on linear problem solvers, which can sometimes falter when confronted with higher complexities. The quantum approach could potentially excel in this regard, having the horsepower to handle high-dimensional problems at greater scale.

HBSC has been at the forefront of exploring the application of quantum technologies in the financial sector.

In July it became the first bank to join BT and Toshiba's quantum-secured metro network - connecting two UK sites using Quantum Key Distribution (QKD) to prepare its global operations against future cyber threats.

The bank has also struck a multi-year deal with IBM to investigate the technology and is actively recruiting research scientists to build a dedicated capability within its innovation team.

In June, it also embarked on a long-term partnership with Quantinuum, the self-described world's largest quantum computing company, with an initial focus on cybersecurity.

22.SK Broadband launches hybrid quantum security service

by Seung-Woo Lee
https://www.kedglobal.com/tech,-media-telecom/newsView/ked202309060009

South Korean internet service provider SK Broadband on Tuesday (05 Sep 2023) said it launched the country's first dedicated line service that supports the online security methods of quantum key distribution (QKD) and post-quantum cryptography (PQC).

Largely divided into QKD and PQC, quantum safe communication (QSC) uses the principle of the quantum trait of uncertainty and that of non-replication.

QKD is a hardware method of using QKD devices that the sender and receiver each have. Its key characteristic is that it is physically impossible to hack.

Based on a mathematical algorithm, PQC is cheaper and more scalable than QKD because of its usability with software. The two technologies complement each other in performance and cost-effectiveness.

Customers can select and use either QKD and PQC, whichever is appropriate for a situation. SK Broadband said a dedicated QKD line with excellent security is suitable for large clients like government and public agencies, medical centers and financial institutions while a PQC, which needs no separate equipment installed, is good for small and medium businesses.

Combining the two QSC methods is also possible. For a bank's biometric authentication security, QKD technology is used in the bank's internal data center and that of PQC is applied between a customer's smartphone and the authentication server to protect biometric information.

In cooperation with SK Telecom Co., SK Broadband received certification from the Korea Cryptographic Module Validation Program for its new service.

23.Bank of Canada explores impact of quantum computing on CBDCs

https://www.finextra.com/newsarticle/42892/bank-of-canada-explores-impact-of-quantum-computing-on-cbdcs

The Bank of Canada has called in local specialist evolutionQ for a research project involving quantum-safe cybersecurity technologies for greenfield digital currencies.

The Bank of Canada is exploring technologies and technical ecosystems that may inform decisions relating to the development of a potential digital loonie.

The evolutionQ research will explore the impact of integrating quantum-safe encryption methods and crypto-agility as design goals for digital currencies.

The code developed during the research will be released as open source to give developers and researchers the opportunity to explore the new cryptographic methods and propose improvements or modifications, accelerating the development of quantum-safe technologies.

Michele Mosca, CEO, evolutionQ, says: "Quantum computing offers great potential to the advancement of many future financial products, but quantum computers also pose new security risks, and it is important to research and build systems that are able to adapt to a quickly shifting threat landscape."

24.Arqit launches the world's first integrated solution for quantum-safe VPN connectivity using Symmetric Key Agreement

https://www.prnewswire.com/news-releases/arqit-launches-the-worlds-first-integrated-solution-for-quantum-safe-vpn-connectivity-using-symmetric-key-agreement-301917780.html

Arqit Quantum Inc. (“Arqit"), a leader in quantum-safe encryption, today announces the availability of the world's first integrated solution for quantum-safe VPN communications.

Arqit's QuantumCloud™ is the world's first fully scalable cloud-based symmetric key agreement platform, capable of creating zero trust quantum-safe encryption keys at any device. By integrating QuantumCloud™ with Juniper Networks® vSRX Virtual Firewall, the resulting solution enables quantum-safe encrypted connectivity between customer locations, keeping data safe both at rest and in transit. Arqit's QuantumCloud uses unique symmetric key agreement software to provide quantum-safe keys which are used by Juniper SRX devices during the formation of secure tunnels.

Juniper's vSRX Virtual Firewall supports the ETSI 014 standard and RFC8784 for IPsec, resulting in the

first GA product supporting flexibility and scalability in generating and using symmetric keys from various sources, including Arqit's symmetric keys.

David Williams, Arqit Founder, Chairman and CEO said, "It is an honour to work with Juniper. We're excited to leverage our integration to deliver enhanced protection against sophisticated cyber attacks of today and tomorrow. In conjunction with Juniper's vSRX Virtual Firewall, our strong, simple encryption enables governments and enterprises to realise enhanced protection against cyber threats and to take a major step forward in significantly reducing the quantum threat from their risk registers."

Samantha Madrid, Group Vice President, Security Business and Strategy at Juniper Networks said, "Juniper is thrilled to be working with Arqit through our technology alliance to enable quantum-safe encrypted connectivity using the QuantumCloud Platform. It is imperative that innovation efforts continue in cybersecurity as threats continue to proliferate in tandem with the pace of digitalisation. Juniper and Arqit are paving the way for safe and reliable cybersecurity solutions to deliver the best experience for organisations and businesses.

25.DT beefs up quantum research to protect networks from qubit-computer attacks

by Ken Wieland
https://www.telcotitans.com/deutsche-telekomwatch/dt-beefs-up-quantum-research-to-protect-networks-from-qubit-computer-attacks/7115.article

Deutsche Telekom has opened a new *Quantum Lab* in Berlin. The lab's brief is to develop quantum cryptography for "*ultra-secure communication*", which can be integrated into current commercial networks, as well as to improve network latency, throughput, and resilience.

Mention was made too of a so-called "quantum Internet of Things", given that quantum entanglement "offers the possibility of more powerful networks of distributed and sensory applications".

The Technical Universities of Berlin, Dresden, and Munich, as well as the Fraunhofer Institut HHI, were name-checked by DT as "*partners*", although there are others involved "*from across academia and business*".

The new research facility, asserted DT, is sufficiently equipped with space and infrastructure for quantum optical experiments. The lab is connected to a 2,000km-plus fibre-optic network, which apparently connects to all T-Labs' quantum research partners in Germany.

In prepared remarks, Claudia Nemat, DT's Chief Technology and Innovation Officer, said the opening of the *Quantum Lab* shows the Group is "*serious*" about bringing quantum technology to telcos' networks.

"We explicitly invite the research and innovation community to join us in leveraging networks at the interface between R&D and commercial exploration like ours. To prove that innovative quantum technology solutions work under real-world conditions, and to usher in a new era of communications service." — Nemat.

Security first

In a short video talking about the *Quantum Lab*, Nemat's main concern appeared to be related to beefing up network security, rather than improving network performance. She voiced a growing industry fear that quantum computing might become too powerful, too soon, before adequate network security countermeasures are developed.

Current public key cryptosystems, according to one BT expert, will be quickly hacked, perhaps in a matter of hours, by future computers that have in excess of 1,000 "*genuine and fully entangled qubits [quantum bits]*".

Nemat said the lab is testing three approaches to fend off hacking attacks by quantum computers. The first is post-quantum cryptography, which relies on algorithms too complex for quantum computers to crack.

Second is quantum key distribution, where distribution of cryptographic keys is done in spatially separated locations, where the exchange of keys cannot be intercepted undetected. "*A potential attacker*", said Nemat, "*would measurably disrupt the exchange process*".

Third is physical layer encoding, which is being tested for the protection of mobile networks.

"We add noise to the signal on purpose. The legitimate receiver can correct it but the potential attacker can't. It can resist attacks from quantum computers." —Nemat

Quantum ramp-up

Deutsche Telekom has announced involvement in various quantum initiatives this year. These include:

- **February**: appointed to lead *PETRUS*, the coordination and support action element of the *European Communication Infrastructure* (*EuroQCI*) project. DT will work to enable public–private collaboration across the 27 member states, with partners Airbus Defence and Space, the Austrian Institute of Technology, and Thales SIX. "*Experts*" from science and industry will also contribute. As coordinator, DT will lead the drive to implement a fully functional quantum network online by 2027. "*This close alignment is required to define shared technical standards and ensure seamless interoperability*", the operator noted.

- **April**: T-Systems, DT's enterprise arm, partnered with IBM to offer its customers cloud-based access to quantum computing services. Access to several quantum computers will be made available, powered by IBM's *Eagle* quantum processor. T-Systems is to offer dedicated training for using the computers, as well as various "*customisable*" quantum services packages, ranging from one-day introductory sessions to support for developing business proof of concepts over several months.

- **July**: T-Systems signed an MoU with IQM Quantum Computers to offer access to cloud quantum computing services and training, with a Europe-based focus.

26.Post Quantum Cryptography Is on the Way: U.S. NIST Announces First Draft Standards

by Michela Menting
https://www.spiceworks.com/it-security/security-general/guest-article/post-quantum-cryptography-first-draft-standards-by-nist/

Post-quantum cryptography (PQC) has passed another milestone. The U.S. National Institute of Standards and Technology (NIST) announced on August 24, 2023, the first draft standards for PQC. Michela Menting of ABI Research explains the standards announced and how they'll affect our evolving tech space.

NIST selected three of the four candidate algorithms it announced back in July 2023 and developed draft standards that it has published with a request for comments. The standards are:

- FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism StandardOpens a new window , based on CRYSTALS-Dilithium
- FIPS 204, Module-Lattice-Based Digital Signature StandardOpens a new window , based on CRYSTALS-KYBER
- FIPS 205, Stateless Hash-Based Digital Signature StandardOpens a new window , based on SPHINCS+

The deadline for comments is November 22, 2023. NIST is currently still in the process of developing a Federal Information Processing Standards (FIPS), leveraging the fourth candidate algorithm (which is a digital signature algorithm), FALCON.

The announcement is an important one on the road to integrating quantum-safety in modern information and communication infrastructure. Since the NIST standardization process began in 2017, the developments in quantum computing have advanced significantly, which has prompted both governments to dictate policy on the matter and for the industry sector to start organizing on the risk assessment front.

Are We Quantum-ready?

From a commercial implementation perspective, the world is far from quantum-ready. While attack-capable quantum computers are expected by 2030 (at the earliest), the transition to post-quantum is likely to take at least a decade. For this reason, standardization efforts (and, in particular, those by NIST) are key in driving industry adoption. But NIST is only the first step in that transitional effort. The role of other Standards Development Organizations (SDOs), such as the Internet Engineering Task Force (IETF), ETSI (European Telecommunications Standards Institute), and the ITU (International Telecommunication Union), is equally important in defining protocols and recommended implementations for various applications.

In parallel, development efforts within specific industry fora and consortia will follow, alongside open-source movements. These will largely leverage SDO standards and recommendations to optimize their

own specifications and reference architectures. The progress of work in these will be a sign of technology maturity and present "plug-and-play" types of technologies, which will make for easier industry integration and adoption.

The standard development process is an intractable and foundational process for the successful development of a PQC market and for eventual adoption and integration into Information and communication technology (ICT). Some industries have been more proactive in engaging with and strategizing around PQC developments, particularly those stakeholders in industries where products have long life spans (10+ years). Automotive original equipment manufacturers (OEMs) are a good example; modern cars are increasingly software-defined and connected, and current product development must look to integrating quantum safeguards today. This has a knock-on effect on the supply chain, notably semiconductors that need to ensure that the chipsets they are providing today can include some form of PQC readiness.

In a similar scenario are highly regulated and highly sensitive markets, such as financial services, defense, and telecommunications. Currently, the risks facing industries may seem minimal, as attack-capable quantum computers are not yet commercially available. However, there are threat actors that are actively stealing encrypted data, with a view to decrypting it later once such computers are available. The risks are, in fact, immediate. The level of preparedness in these industries varies significantly, and is also affected by whether there is any government policy in their geographic region.

There are varying reasons for this fragmentation in approach. In large part, the issues center around the complexity of PQC-based key exchange and the difficulty in making the schemes practicable for a broad range of applications. It's not a one-size-fits-all solution. Therefore, efforts in industry consortia are key.

The Need for a Unified Approach to Standards

Further adding to the complexity is the fact that there will be several different standards based on different algorithms. This is a big change in the cryptographic world, which had only to deal with one new cryptographic algorithm in the last decade (elliptic curve cryptography (ECC)). Fewer standards would be better for migration, but there is a need for different algorithms based on application and final usage.

There is also the challenge around public awareness, which, in general, has not been so high-profile outside of the security industry. Because quantum computing is still mostly theory, PQC is not a priority topic for many. Its importance has not been conveyed successfully enough to generate a high level of interest outside a very niche audience despite the apparent risks.

Finally, the rationale for many is to wait until finalized standards and commercial off-the-shelf solutions are available. There is anxiety about the cost of implementing PQC too early; what if one of the standards is broken in the next year? What if attack-capable quantum computers don't emerge for another 20 years? Is that spending justifiable? And there are other pressing priorities, such as ransomware and supply chain attacks, where security budgets could be better spent.

The Time to Think About PQC Is Now

At worst, there are those who will simply wait for attack-capable quantum computers to be commercially viable before thinking about PQC at all. This would be a mistake.

Nonetheless, progress by NIST and the IETF shows that PQC is not some theoretical concept that can be easily ignored. The various efforts have engaged some of the world's largest and most influential technology and security companies for years now (see the figure below).

The integration of PQC will absolutely permeate their product lines and solutions, democratizing PQC understanding and awareness in the process. While still incipient (even after five years), a long and involved process remains, from standards development to ubiquitous integration.

27.The quantum threat: Implications for the Internet of Things

by Jonathan Lane
https://www.computerweekly.com/opinion/The-quantum-threat-Implications-for-the-Internet-of-Things

With an estimated 43 billion Internet of Things (IoT) devices expected to be in use globally in 2023, their security is growing in importance across a wide range of sectors. As IoT devices generate and exchange data, we depend on that data to be accurate and reliable. In addition, because they are networked, their exploitation can open attack vectors in wider systems which could result in extensive and global impact.

In 2016 the largest ever botnet attack was launched on the service provider Dyn using the Mirai malware. This malware looked for IoT devices running the Linux ARC operating system, attacked them with default login information and infected them. This enabled huge numbers of IoT devices to be used together in distributed denial of service (DDoS) attacks resulting in significant parts of the internet going down.

Another example was the Medtronic Insulin Pump Vulnerability. In 2019 it was found that some Medtronic MiniMed insulin pumps had vulnerabilities in their Wi-Fi connectivity, making it possible for an unauthorised person to control the pump with potentially life-threatening consequences.

IoT devices tend to be on smaller platforms that have technical limitations on their space, weight and power. As a result, they have lower processing capacity and cannot run sophisticated authentication and cryptographic solutions. In addition, many of our current IoT devices are poorly architected and badly configured when installed meaning that security measures are often not operational. When you integrate these smart devices into a network that also has much older and simpler devices, the potential for impact scales considerably.

Many organisations are working hard to get the security basics in place and recognise that they have an issue. However, getting businesses to invest in longer term IoT security is often a significant challenge.

Quantum computing, though it might be a decade or two away, presents a threat to IoT devices that have been secured against the current threat and which may remain in place for many years. To address

this threat, governments are already spending billions, while organisations like NIST and ETSI are several years into programmes to identify and select post-quantum algorithms (PQAs) and industry and academia are innovating. And we are approaching some agreement on a suite of algorithms that are probably quantum safe; both the UK's NCSC and the US' NSA endorse the approach of enhanced Public Key cryptography using PQA along with much larger keys.

The NCSC recommends that the majority of users follow normal cyber security best practice and wait for the development of NIST standards-compliant quantum-safe cryptography (QSC) products. That potentially leaves the IoT with a problem. Most of these enhanced QSC standards appear to require considerable computing power to deal with complex algorithms and long keys – and many IoT sensors may not be capable of running them.

So until NIST delivers its QSC standards we won't know whether they will work within IoT constraints. If they don't, then there is a gap in the formal development of IoT QSC solutions.

This is a fast-moving area with a lot of innovation so it may make sense to look elsewhere for alternative viable solutions.

Asymmetric cryptography, for example, could be viable with low resource PQC algorithms. Symmetric cryptography is currently favoured by the IoT industry as a low-power mechanism, but the problem of secretly distributing the same keys to each party remains and quantum enhancements may push up power requirements. Then there are symmetric key establishment mechanisms where innovation may help, as there are alternative approaches being considered.

These include quantum key distribution (QKD) which uses the properties of quantum mechanics to establish a key agreement, rather than using difficult mathematical problems that quantum computers will solve quickly. However, QKD requires specialist hardware, and does not provide a way of easily enabling authentication, and the NCSC does not endorse QKD for any government or military applications.

Another option is secure key agreement (SKA). Some companies are experimenting with computationally safe ways of digitally creating symmetric keys across trusted endpoints. This type of low-power, software based capability offers an interesting alternative for the IoT. But although independent verification of this type of capability is happening, this approach is neither on NIST's nor ETSI's radar.

Conclusions

Most IoT applications are not facing an immediate quantum computing threat. However, the IoT estate is vulnerable to standard computing threats and there appears to be a lack of commitment to do much about this.

If we are to equip our increasingly connected IoT world for the quantum threat, then we need to take three actions. The first is to foster a security-conscious culture among users, and to embed IoT security as standard practice. The second is to urge manufacturers to adhere to established security standards, ensuring that devices are inherently secure by design. Finally research into low-resource quantum-safe solutions must intensify, and we should embrace the development of novel approaches.